EXHIBIT G

CITATION: Del Giudice v. Thompson, 2021 ONSC 5379
COURT FILE NO.: CV-19-00625030-00CP
DATE: 20210804

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:	
RINA DEL GIUDICE and DANIEL WOOD Plaintiffs	*John A. Campion*, *R. Douglas Elliott*, *Glyn Hotz* and *Darrel N. Hotz* for the Plaintiffs
- and -	
PAIGE A. THOMPSON, CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (CANADA BRANCH), CAPITAL ONE (SERVICES) CANADA INC., CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., GITHUB, INC., AMAZON WEB SERVICES INC., AND AMAZON WEB SERVICES (CANADA) INC. Defendants	*Laura F. Cooper*, *Sarah J. Armstrong*, *Alex D. Cameron*, *Vera Toppings* and *Pavel Sergeyev* for the Defendants Capital One Financial Corporation, Capital One Bank (Canada Branch), Capital One (Services Canada Inc., Capital One, N.A., Capital One Bank (USA), N.A. *Scott Kugler*, *Brent J. Arnold*, *Elie Laskin* and *Kavi Sivasothy* for the Defendants Amazon Web Services Inc., and Amazon Web Services (Canada) Inc.
Proceeding under the *Class Proceedings Act, 1992*	**HEARD:** June 7-9, 2021

PERELL, J.

REASONS FOR DECISION

A. Introduction and Overview

[1] This is a certification motion in a $10.9 billion data breach case that Class Counsel has redesigned into a $240 billion data misappropriation and misuse case.

[2] In this proposed class action under the *Class Proceedings Act, 1992*,[1] it is alleged that on March 22 or 23, 2019, the Defendant Paige Thompson hacked the data base of personal

[1] S.O. 1992, c. 6.

information collected by the Defendants Capital One Financial Corporation, Capital One, N.A., Capital One Bank (USA), N.A., Capital One Bank (Canada Branch), Capital One Services Canada Inc., (collectively "Capital One") from American and Canadian citizens. The Capital One data was stored on the computer servers of the Defendants Amazon Web Services Inc., and Amazon Web Services (Canada) Inc. (collectively "Amazon Web"). Ms. Thompson misappropriated the data. She posted the data on the website of the Defendant GitHub, Inc., which provides a forum for software developers to share information. As a consequence of this data breach, personal and confidential information of 106 million applicants for Capital One credit cards was exposed or became vulnerable to exposure to the public. It is estimated that approximately six million Canadians were affected.

[3] On August 6, 2019, Rina Del Giudice commenced a proposed Canadian class action with respect to the data breach. Subsequently, Daniel Wood became a co-Plaintiff. The action was recently discontinued as against GitHub.[2]

[4] Class Counsel are a consortium: (a) Gardiner Roberts LLP; (b) Cambridge LLP; (c) Hotz Lawyers; and (d) Scher Law Professional Corporation. The consortium brands itself as "PDBL – Privacy and Data Breach Law Group." The lead counsel is John A. Campion. On April 30, 2020, the consortium was granted carriage of the proposed class action.[3]

[5] The Plaintiffs now bring a motion to have their action certified as a class action.

[6] On August 27, 2020, I directed that the certification motion have two phases. Phase I was to determine whether and the extent to which the Plaintiffs have satisfied the cause of action criterion, the first of the five statutory criteria that must be satisfied for an action to be certified as a class proceeding.

[7] In Phase I, the Defendants assert that none of the nineteen pleaded causes of action are certifiable. They submit that the Plaintiffs have not properly pleaded any recognized causes of action. For several causes of action, the Defendants submit that constituent elements are missing. They submit other causes of action are not known to the law. The Defendants recognize that several of the pleaded causes of action are novel, but the Defendants submit that these novelties should be struck because they go beyond the incremental development of the common law. The Defendants submit that all of the causes of action should be struck without leave to amend.

[8] For the reasons that follow, I conclude that the Plaintiffs' Fresh as Amended Statement of Claim should be struck out in its entirety without leave to deliver a Second Fresh as Amended Statement of Claim.

[9] Although a considerable amount of analysis will be required to explain my decision, a simple overview of my reasoning is that the Plaintiffs' Fresh as Amended Statement of Claim should be struck out in its entirety for at least three discrete reasons, two of which are mundane, and the third of which is ironic in the circumstances of this undoubtedly important case.[4]

---

[2] *Del Giudice v. Thompson*, 2021 ONSC 3696 [GitHub discontinuance] and *Del Giudice v. Thompson*, 2021 ONSC 4024 [re GitHub settlement].

[3] *Del Giudice v. Thompson*, 2020 ONSC 2676 [carriage mtn].

[4] While the case is an important one, Mr. Campion exaggerated its importance. He submitted that the privacy rights and the *Charter* rights of Canadian citizens have been put at risk by the intimidating and illegal acts of the Defendants, which must be stopped. He said that the failure of financial institutions and internet providers such as the defendants to provide data protection to customers was an existential threat to the entire financial system in

[10] First, the Plaintiffs' Fresh as Amended Statement of Claim should be struck out because it egregiously contravenes the rules of pleading.

[11] Second, the Plaintiffs' Fresh as Amended Statement of Claim should be struck out because it is plain and obvious that the Plaintiffs failed to plead any legally viable causes of action against Capital One and Amazon Web.

[12] Third, the Plaintiffs' Fresh as Amended Statement of Claim should be struck out because in an irony in a case about computer technology, it was revealed that after the carriage motion and months of graduate school learning about law and technology, Mr. Campion decided to transform the Plaintiffs' straightforward data breach case into a data misappropriation and misuse case. It was revealed during oral argument that he had not developed a legal theory to fit the facts. Rather, he developed what I shall label a legal logarithm that would invariably and inevitably achieve victory for the Class Members, whatever the material facts might be.

[13] I was informed during oral argument that if the Plaintiffs' action could just be allowed to proceed, then Class Counsel's legal theory would achieve victory regardless of the factual inputs of the known material facts (constants) and all the presently unknown material facts (variables). The variables could and would become known material facts after the Defendants had produced their documents and been examined for discovery or cross-examined for a summary judgment motion.[5] However, pursuant to the legal theory, whatever the material facts would be, the Defendants would be liable. Resistance was futile and the case must be certified in order for access to justice to be achieved and the evildoing stopped.

[14] The legal theory of the case was filed in a 56-page compendium that arrived the day before Phase I was argued. The flow chart from this legal logarithm is attached as Schedule "B" to these Reasons for Decision. However, all that Class Counsel achieved by filing the compendium is a third reason to strike the Fresh as Amended Statement of Claim.

[15] For these reasons and more to follow, the Plaintiffs have advanced a case that is doomed to fail and their Fresh as Amended Statement of Claim should be struck out without leave to amend. I dismiss the Plaintiffs' certification motion. I lift the stay of other proposed class actions that I imposed when I granted carriage to the Plaintiffs' consortium of Class Counsel.

B. Methodology

[16] After the above Introduction and Overview (Part A) and this explanation of the methodology for the Reasons for Decision (Part B), I shall explain the reasons for my dismissal of the Plaintiffs' motion in the following way.

[17] In Part C, I shall discuss what was an unpleasant and contentious preliminary matter. I shall

---

Canada. He said that intrusion on seclusion and several new or extended causes of action can be and must be applied in the circumstances of the immediate case to restore the guardrails that prescribe the use of private and confidential information. He said that the world is watching the outcome of this case. He said that the case was more important than the repatriation of the Canadian Constitution. He said that the use of personal information, which has been made extraordinarily valuable by the advances in computer technology must be regulated by the civil law (common law and statutes) to protect against the invasion and destruction of privacy and along with it the end of liberal democracy.

[5] Borrowing from the late Donald Rumsfeld, former American Secretary of Defence, Mr. Campion said that the legal theory of the case would accommodate "known knowns", "known unknowns", and the "unknown unknowns".

discuss Capital One's filing of contract documents and the Plaintiffs' protest and request for a sealing order.

[18] In Part D, I shall discuss the rules of pleading and their application to the Plaintiffs' Fresh as Amended Statement of Claim and I shall explain why the pleading should be struck out in its entirety.

[19] In Part E, I shall set out without commentary the pertinent excerpts from the contract documents incorporated by reference in the Plaintiffs' Fresh as Amended Statement of Claim; namely: (a) Capital One's Privacy Policy; (b) its Application for Credit; and (c) its Credit Card Agreement.

[20] In Part F, I shall describe the material facts that may be extracted from the Plaintiffs' Fresh as Amended Statement of Claim. I shall also summarize and contrast the factual narratives of the data breach case and the data misappropriation and misuse case.

[21] In Part G, I shall list the pleaded causes of action and I shall set out the legal principles that govern the first criterion for certification in a proposed class action.

[22] In Parts H through P, I discuss the Plaintiffs' various pleaded causes of action in the following order: Intrusion upon Seclusion (Part H); Misappropriation of Personality (Part I); Privacy Statutes (Part J); Conversion (Part K); Breach of Trust and Breach of Fiduciary Duty) (Part L); Strict Liability (Part M); Vicarious Liability (Park N); Negligence and Duty to Warn (Part O); and, Breach of Contract/Negligent Breach of Contract (Part P).

[23] In Part Q, I shall describe the Plaintiffs' Legal Theories and what I have described as Class Counsel's legal logarithm for advancing claims against Capital One and Amazon Web.

[24] Part R is the Conclusion and my treatment of the matter of costs.

C. The Filing of Contract Documents and the Matter of the Sealing Order

1. The Regrettable Procedural Saga of the Contract Documents.

[25] Although I am disheartened to have to do so, I must discuss the procedural saga of the contract documents that underpin all of the Plaintiffs' causes of action. These documents are central to the story of what happened to the Class Members' personal information that Capital One collected from persons, like the Plaintiffs and the six million Canadians who applied for Capital One credit cards. Notwithstanding their centrality, there was a bitter dispute about the admission of the documents and their use on the motion.

[26] In this part of my Reasons for Decision, I shall explain: (a) why the contract documents could and should be referred to on this motion; (b) why Capital One's and Amazon Web's conduct in filing the contract documents was proper; (c) why Senior Class Counsel's critical comments about the conduct of Sarah Armstrong, counsel for Capital One, and of Scott Kugler, counsel for Amazon Web, were and are without merit; and (d) why I shall not make a sealing order.

2. The Saga of the Filing of the Document Brief

[27] The procedural background to the matter of the filing of the Document Brief begins on August 27, 2020, when I directed that the certification motion have two phases. Phase I was to

determine whether and the extent to which the Plaintiffs have satisfied the cause of action criterion.

[28] In October 2020, the Plaintiffs filed their six volume, 5,000-page motion record. The motion record contained the Plaintiffs' Fresh as Amended Statement of Claim. The pleading advances a breach of contract claim and a negligent breach of contract claim on behalf of at least some Class Members. As confirmed during oral argument and Box 20 in the Plaintiffs' Compendium, the contract claim is referred to in thirty paragraphs of the Fresh as Amended Statement of Claim.[6]

[29] The Certification Motion Record included an affidavit from Ms. Del Giudice. She deposed that she was the holder of a Capital One credit card that was subject to the 2019 data breach. She deposed that she was not aware of or informed of the uses made of the personal information contained in her credit card application. She deposed that she had provided personal information within the context of a Canadian credit card application and for that purpose only. She deposed her qualifications to be a Representative Plaintiff.

[30] Although it was the source of her grievances and the grievances of the Class Members, the voluminous Certification Motion Record did not contain a copy of Ms. Del Giudice's credit card application or her credit card agreement with Capital One.

[31] In October 2020, the Plaintiffs also filed their Factum for Phase I of the Certification Motion.

[32] Four months passed, and on March 1, 2021, GitHub, Amazon, and Capital One respectively filed their Responding Factums for Phase I.

[33] In paragraph 6 of its Responding Factum, Capital One stated:

> [the Plaintiffs], having pleaded the existence of, and breaches of, the Plaintiffs' contracts with Capital One, those documents are incorporated by reference into, and become part of, the Fresh as Amended Statement of Claim, and must be considered in determining whether the Plaintiffs have pleaded viable causes of action."

[34] Along with its Responding Factum, Capital One filed a Document Brief containing its Privacy Policy, Ms. Del Giudice's Application for Credit, and a Credit Card Agreement. Capital One did not seek leave of the court to file the Document Brief. It did not seek a sealing order. Capital One referred to these documents in its Responding Factum on the basis that the documents had been incorporated by reference in the Plaintiffs' Fresh as Amended Statement of Claim.

[35] On April 23, 2021, the Plaintiffs delivered their Reply Factum for Phase I of the Certification Motion. In the Plaintiffs' Reply Factum, no objection was taken to Capital One's having referred to the contract documents and to its Privacy Policy in its Responding Factum.

[36] Two months passed. Phase I was scheduled to begin on June 9, 2021, and in May and June, I dealt with the matter of the discontinuance of the action as against GitHub and several other procedural matters that need not be recounted for present purposes. In preparing for Phase I of the certification motion, I read the parties' factums. From the Document Brief, I read in their entirety Capital One's Privacy Policy, Application for Credit, and its Credit Card Agreement.

[37] On the morning of June 9, 2021, I received an email request from Ms. Armstrong, one of

---

[6] Fresh as Amended Statement of Claim paragraphs 1(c)(e), 4, 11, 18, 31, 38(viii)(x), 41, 54, 58, 76, 81, 82, 84, 82, 98, 101, 102, 103, 104, 106, 107, 109, 111, 113, 114, 116, 117, and 128.

Capital One's lawyers, to schedule an emergency case management conference to deal with a problem that had emerged over the weekend with respect to Capital One's Document Brief.

[38] On June 9, 2021, after hearing some submissions from the parties, I treated the case management conference as a preliminary motion and Phase I got underway. There was an uproar about the Document Brief.

[39] Ms. Armstrong told me that over the weekend, Mr. Campion had objected to her filing of the Document Brief as improper and as a breach of Ms. Del Giudice's privacy and of the *Rules of Civil Procedure*.[7] She denied impropriety, but said, however, that the brief had never been filed in the court file and that she had withdrawn the documents from https://ontariocourts.caselines.com, where the brief had been filed for the purposes of the hearing of Phase I. She said that she had offered to refile a redacted version of the documents, but Mr. Campion had declined this solution.

[40] Mr. Campion submitted that the filing of the Document Brief was an abusive act meant to intimidate him personally and to intimidate and embarrass Ms. Del Giudice and to scare her from proceeding with her class action. He submitted that the filing of the Document Brief was a breach of privacy by Capital One's and Amazon Web's lawyers and another invasion of privacy by Capital One and Amazon Web. He said that the Defendants' lawyers had breached their duties as officers of the court by filing the documents without court approval and without the documents being under seal. He said the Defendants' lawyers had improperly attempted to convert a pleadings motion into a summary judgment motion. He said that he had not appreciated until the week before the motion, when he began his preparation for the argument, that Capital One and Amazon Web had filed Ms. Del Giudice's credit application that contained confidential information about her occupation, her income, and her SIN number. He said the Defendants knew and had acknowledged that this information was confidential personal information. He said that the documents should not have been unilaterally filed without a sealing order and a direction from the court. He objected to the filing and unilateral use of the Document Brief. He asked the court to make a direction that the documents were not admissible. He said that the court should chastise the Defendants and their lawyers for their intimidating conduct and breaches of confidence. He said that he was entitled to cross-examine and have the authenticity of the documents and Ms. Del Giudice's signature proven. He said that he is entitled to have this case tried and that it would be egregiously unfair to allow the Defendants to turn a pleadings motion into a summary judgment motion based on contract documents that have never been proven and that were not referred to in the Plaintiffs' pleadings. He said that if the court directed that the documents were accepted, then he would proceed under protest. He said that, in any event, the filing of the documents was a fatal mistake by Capital One and Amazon Web because the filing was both an admission of wrongdoing and a demonstration that these Defendants had violated the privacy of Ms. Del Giudice once again. He said that while he objected to the filing of the contract documents, he would capitalize on their filing to show that his clients had numerous viable causes of action.

[41] After hearing Mr. Campion's submissions, I did not call on Ms. Armstrong to reply, and I directed that the Document Brief could be used on the certification motion. After my direction, Mr. Campion said he would proceed under protest, and he asked that the Document Brief be sealed. Ms. Armstrong said that she would seek instructions, and later in the hearing, she advised that Capital One did not oppose a sealing Order.

---

[7] R.R.O. 990, Reg. 194.

3. The Treatment of the Document Brief

[42] This being the factual background, my analysis and conclusions are as follows.

[43] As I shall discuss further later in these Reasons for Decision, the contract documents in the Document Brief were incorporated by reference into the Fresh as Amended Statement of Claim.

[44] Capital One did not convert a pleadings motion into a summary judgment motion; it filed documents that were incorporated in a pleading by reference, and this type of filing is a normal event on a pleadings motion.

[45] There was nothing improper and nothing nefarious in Capital One filing the Document Brief. Amazon Web had nothing to do with this filing, but it was entitled to rely on what is a normative accordance on a certification motion and is a routine matter that has occurred on thousands if not hundreds of thousands of Rule 21 pleadings motions to challenge the legal viability of a cause of action, when the statement of claim makes a claim in contract.

[46] It is commonplace on certification motions for plaintiffs to file the contract documents that are relevant to their causes of action. But for the fact that the certification motion in the immediate case was bifurcated, Capital One's contract documents and, in particular, the application form, which is the source of Class Members' grievances, would normally have been produced for the certification motion.

[47] Capital One's filing of the Document Brief is not an admission of what is or is not confidential information or admission about what documents should be sealed. These filings are not admissions, new breaches of contract, or new invasions of privacy. They were proper filings of materials for the purposes of motions before the court.

[48] If there is something beyond obviousness, it is that Ms. Del Giudice's application form was incorporated by reference in her Fresh as Amended Statement of Claim. If Ms. Del Giudice had a right of privacy or confidentiality with respect to those documents, she waived it when she decided to be the champion for the other Capital One cardholders and sue for $240 billion. I do not believe that she or Mr. Campion were intimidated in the least by the filing of the Document Brief. If Ms. Del Giudice is genuinely scared to proceed, then she is not qualified to be a representative plaintiff notwithstanding her affidavit in the Certification Motion record that deposes her championing qualities. Ms. Del Giudice is suing to recover $240 billion, and she has experienced battle-hardened lawyers to protect her for the legal warfare that befits such a prize. For present purposes, I assume that she is up to the task and will not be intimidated.

[49] Mr. Campion's submission that there was unprofessional or improper conduct by Ms. Armstrong or Mr. Kugler is without a scintilla of merit. The filing of the contract documents was not a breach of privacy. Capital One was filing documents that ought to and normally would have been filed by Class Counsel on a certification motion. Ms. Armstrong and Mr. Kugler were professional in providing a defence of their clients who were being sued for $240 billion and whose liability remains to be determined.

[50] Save for the matter of redacting the SIN number and the amount of Ms. Del Giudice's income, there was nothing that would remotely justify a sealing order in the immediate case. I simply direct that Capital One file the Document Brief with personal information redacted.

D. The Rules of Pleading and the Fresh as Amended Statement of Claim

[51] As noted above, the Plaintiffs' Fresh as Amended Statement of Claim is set out in the annexed Schedule "A." For the following reasons, I strike out the pleading it its entirety for violating the rules of pleading.

1. The Rules of Pleading

[52] Rule 25.06 (1) of the *Rules of Civil Procedure* directs that every pleading shall contain a concise statement of the material facts on which the party relies for the claim or defence, but not the evidence by which those facts are to be proved. A pleading should be brief, clear, focused and contain the skeletal or core facts and not the evidence that details those facts unless particulars are required by the rules.[8]

[53] Material facts include facts that the party pleading is entitled to prove at trial, and at trial, anything that affects the determination of the party's rights can be proved; accordingly, material facts includes facts that can have an effect on the determination of a party's rights.[9] A fact that is not provable at the trial or that is incapable of affecting the outcome is immaterial and ought not to be pleaded.[10] A pleading of fact will be struck if it cannot be the basis of a claim or defence and is designed solely for the purposes of atmosphere or to cast the opposing party in a bad light.[11] As described by Riddell J. in *Duryea v. Kaufman*,[12] such a plea is said to be "embarrassing".

[54] "Material" facts include facts that establish the constituent elements of the claim or defence.[13] The causes of action must be clearly identifiable from the facts pleaded and must be supported by facts that are material.[14]

[55] A pleading shall contain material facts, but it should not contain the evidence by which those facts are to be proved.[15] Pleadings of evidence may be struck out.[16] The prohibition against pleading evidence is designed to restrain the pleading of facts that are subordinate and that merely tend toward proving the truth of the material facts.[17]

[56] Under rule 25.11, the court may strike out a pleading that may prejudice or delay the fair

---

[8] *Mudrick v. Mississauga Oakville Veterinary Emergency Professional Corp.*, [2008] O.J. No. 4512 (Master).
[9] *Brydon v. Brydon*, [1951] O.W.N. 369 (C.A.); *Hammell v. British American Oil Co.*, [1945] O.W.N. 743 (Master); *Daryea v. Kaufman* (1910), 21 O.L.R. 161 (H.C.J.).
[10] *Wood Gundy Inc. v. Financial Trustco Capital Ltd.*, [1988] O.J. No. 275 (H.C.J.); *Guaranty Trust Co. of Canada v. Public Trustee* (1978), 20 O.R. (2d) 247 (H.C.J.); *Everdale Place v. Rimmer*, (1975), 8 O.R. (2d) 641 (H.C.J.); *Elder v. Kingston (City)*, [1953] O.W.N. 409 (H.C.J.).
[11] *Canadian National Railway Co. v. Brant* (2009), 96 O.R. (3d) 734 (S.C.J.); *Wilson v. Wilson*, [1948] O.J. No. 62 (H.C.J.).
[12] *Duryea v. Kaufman* (1910), 21 O.L.R. 165 at p. 168 (H.C.J.).
[13] *Philco Products, Ltd. v. Thermionics, Ltd.*, [1940] S.C.R. 501.
[14] *Cerqueira v. Ontario*, 2010 ONSC 3954 at para. 11.
[15] *McDowell and Aversa v. Fortress Real Capital Inc*., 2017 ONSC 4791; *Murray v. Star*, 2015 ONSC 4464; *Mudrick v. Mississauga Oakville Veterinary Emergency Professional Corp*., [2008] O.J. No. 4512 (Master).
[16] *Envirochill Cryogen Development Corporation v. University of Ontario Institute of Technology*, 2018 ONSC 766 (Master); *Jacobson v. Skurka*, 2015 ONSC 1699; *Sun Life Assurance Co. of Canada v. 401700 Ontario Ltd.* (1991), 3 O.R. (3d) 684 (Gen. Div.).
[17] *Grace v. Usalkas*, [1959] O.W.N. 237 (H.C.J.).

trial of the action or that is scandalous, frivolous, vexatious or an abuse of process of the court.[18] The same test that is used for striking a pleading for the failure to show a reasonable cause of action; *i.e.*, the plain and obvious test, is used to determine whether a pleading is scandalous, frivolous or an abuse of process of the court.[19]

[57] A claim may be found to be frivolous, vexatious or an abuse of process when it asserts untenable pleas, is argumentative, contains insufficient material facts to support the allegations made, or is made for an extraneous or collateral purpose.[20] For the purpose of rule 25.11, the term "scandalous", includes allegations that are irrelevant, argumentative, simply inserted for colour or to impugn the behaviour or character of the other party unrelated to the issues in the litigation.[21]

[58] Parties are to be allowed a great deal of latitude in how they plead, but there are limits, and the court has the jurisdiction to strike a pleading to remove the pleading of evidence, prolix or vague allegations, repetitive or redundant allegations, or inconsistent allegations that are not clearly pled as alternatives and to direct a party to plead with certainty, precision and with sufficient particulars.[22]

[59] A scandalous pleading refers to indecent or offensive allegations designed to prejudice the opponent or unnecessary allegations maliciously directed at the moral character of the opponent.[23] Pleadings that are irrelevant, argumentative or inserted only for colour, or that constitute bare unfounded allegations should be struck out as scandalous.[24] A pleading that raises an issue that cannot influence the outcome of the action is scandalous.[25] The pleading is struck out because it serves no purpose other than to add colour or argument and to disconcert or humiliate the opponent.[26] References in pleadings to settlement offers, discussions, and negotiations, which are privileged communications, are scandalous, frivolous or vexatious and should be struck from the pleading.[27]

---

[18] *876502 Ontario Inc. v. I.F. Propco Holdings (Ontario) 10 Ltd.* (1997), 37 O.R. (3d) 70 (Gen. Div.); *R. Cholkan & Co. v. Brinker* (1990), 71 O.R. (2d) 381 (H.C.J.); *Demeter v. British Pacific Life Insurance Co.* (1983), 43 O.R. (2d) 33 (H.C.J.), affd (1984), 48 O.R. (2d) 266 (C.A.); *Foy v. Foy*, (1978), 20 O.R. (2d) 747 (C.A.).

[19] *Resolute Forest Products Inc. v. 2471256 Canada Inc. (c.o.b. Greenpeace Canada)*, 2016 ONSC 5398 (Div. Ct.); *Miguna v. Toronto (City) Police Services Board*, 2008 ONCA 799.

[20] *Carney Timber Co. v. Pabendinskas*, [2008] O.J. No. 4818 (S.C.J.); *Hainsworth v. Ontario*, [2002] O.J. No. 1380 (S.C.J.); *Panalpina Inc. v. Sharma*, [1988] O.J. No. 1401 (H.C.J.).

[21] *Holder v. Wray*, 2018 ONSC 6133 (S.C.J.); *Carney Timber Co. v. Pabendinskas*, [2008] O.J. No. 4818 (S.C.J.); *George v. Harris*, [2000] O.J. No. 1762 (S.C.J.).

[22] *Cadieux (Litigation guardian of) v. Cadieux*, 2016 ONSC 4446 (Master); *Dolan v. Centretown Citizens Ottawa Corp.*, 2015 ONSC 2145 (Master); *Fockler v. Eisen*, 2012 ONSC 5435.

[23] *Wolker v. Ogilvie Realty Ltd*., [2006] O.J. No. 381 (S.C.J.); *876502 Ontario Inc. v. I.F. Propco Holdings (Ontario) 10 Ltd.* (1997), 37 O.R. (3d) 70 (Gen. Div.); *Paul v. Paul* (1980), 28 O.R. (2d) 78 (H.C.J.).

[24] *Gardner v. Toronto Police Services Board*, [2006] O.J. No. 3320 (Ont. S.C.J.), var'd 2007 ONCA 489; *Senechal v. Muskoka (District Municipality)*, [2003] O.J. No. 885 (S.C.J.); *Solid Waste Reclamation Inc. v. Philip Enterprises Inc*., [1991] O.J. No. 213 (Gen. Div.).

[25] *Caras v. IBM Canada Ltd*., [2004] O.J. No. 3009 (Master); *Everdale Place v. Rimmer* (1975), 8 O.R. (2d) 641 (H.C.J.).

[26] *Sequin v. Van Dyke* 2011 ONSC 2566 (Master); *Dugal v. Manulife Financial Corp*., 2011 ONSC 387; *Williams v. Wai-Ping*, [2005] O.J. No. 1940 (S.C.J.), aff'd, [2005] O.J. No. 6186 (Div. Ct.); *Jane Doe v. Escobar*, [2004] O.J. No. 2760 (S.C.J.); *Hodson v. Canadian Imperial Bank of Commerce*, [2001] O.J. No. 4378 (Div. Ct.); *George v. Harris*, [2000] O.J. No. 1762 (S.C.J.).

[27] *Lemonius v. Audmet Canada*, 2019 ONSC 4485 (Master*); 2030945 Ontario Ltd. v. Markham Village Shoppes Ltd.*, 2013 ONSC 1020 (Master); *Canadian Gateway Development Corp. v Canada (National Capital Commission)*, [2002] O.J. No. 3167 (Master)

[60] The rule authorizing the court to strike out a pleading as prejudicial, scandalous, frivolous, vexatious, or an abuse of the process of the court is exercised only in the clearest of cases.[28] Where a pleading is struck as defective, leave to amend should only be denied in the clearest cases when it is plain and obvious that no tenable cause of action is possible on the facts as alleged.[29] The usual practice is to grant the plaintiff leave to amend unless it is clear that the plaintiff cannot improve its case by any further and proper amendment.[30]

[61] Where a pleading is overborne by its improperly plead allegations, it should be struck out or amended in its entirety.[31]

2. Striking the Fresh as Amended Statement of Claim

[62] The following paragraphs of the Fresh as Amended Statement of Claim are struck out in whole or in part for the failure to plead a material fact or for including irrelevant and non-material or embarrassing or scandalous facts: 5, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 29, 30, 31, 32, 33, 34, 38, 41, 44, 56, 58, 59, 64, 65, 66, 67, 77, 80, 99, 105, 106, 107, 108, 109, and 112.

[63] The following paragraphs of the Fresh as Amended Statement of Claim are struck out in whole or in part for containing the evidence by which a material fact is to be proved: 14, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 38, 40, 41, 42, 43, 44, 45, 56, 58, 59, 64, 65, 66, 67, 69, 72, 73, 77, 79, 80, 81, 105, 106, 107, 108, and 109.

[64] The following paragraphs of the Fresh as Amended Statement of Claim are struck out in whole or in part as argumentative or as making vague, repetitive, redundant, irrelevant, inconsistent, or scandalous allegations: 10, 16, 17, 18, 19, 20, 21, 28, 30, 31, 32, 34, 38, 41, 43, 44, 45, 46, 49, 50, 51, 52, 53, 54, 55, 56, 58, 59, 60, 62, 64, 66, 68, 71, 72, 73, 74, 75, 76, 77, 78, 79, 82, 85, 86, 93, 98, 100, 101, 104, 105, 106, 107, 108, 109, 111, 112, 113, 128, and 130.

[65] The 134 paragraphs of the Plaintiffs' Fresh as Amended Statement of Claim are overborne by its improperly pleaded allegations in 78 paragraphs of the pleading. The pleading should be struck out in its entirety.

[66] I do not grant the Plaintiffs leave to deliver a Second Fresh as Amended Statement of Claim. No purpose would be served by doing so. In the balance of these Reasons for Decision, I shall determine whether the Plaintiffs satisfy the cause of action criterion based on the current pleading from which I shall extract the material and other facts. As foreshadowed above and discussed in detail below, the Plaintiffs have advanced a case and an approach to a case that is doomed to fail, and thus no purpose would be served by granting the Plaintiffs leave to amend.

E. Capital One's Privacy Policy, Application for Credit, and Credit Card Agreement

[67] In this section of my Reasons for Decision, I set out Capital One's Privacy Policy, a sample of an Application for Credit and a Credit Card Agreement. (I do so without disclosing any personal

---

[28] *Tarion Warranty Corp. v. Brookegreene Estates Inc.*, [2006] O.J. No. 923 (S.C.J.); *Wernikowski v. Kirkland, Murphy & Ain* (1999), 50 O.R. 124 (C.A.).
[29] *Mitchell v. Lewis*, 2016 ONCA 903; *Conway v. Law Society of Upper Canada*, 2016 ONCA 72; *Piedra v. Copper Mesa Mining Corp.*, 2011 ONCA 191; *Heydary Hamilton Professional Corp. v. Hanuka*, 2010 ONCA 881.
[30] *Fournier Leasing Co. v. Mercedes-Benz Canada Inc.*, 2012 ONSC 2752; *AGF Canadian Equity Fund v. Transamerica Commercial Finance Corp. Canada*, (1993), 14 O.R. (3d) 161 (Gen. Div.).
[31] *Cadieux (Litigation guardian of) v. Cadieux*, 2016 ONSC 4446 (Master); *Fockler v. Eisen*, 2012 ONSC 5435.

information about Ms. Del Giudice or Mr. Wood.)

[68] I have **underlined** in bold text for emphasis the portions of the documents that address the matters of: (a) Capital One's responsibilities to protect the Class Members' personal information; and, (b) the extent to which a Class Member may have consented to the use of his or her personal information.

[69] Capital One's Privacy Policy stated:

CAPITAL ONE PRIVACY POLICY

1. PRIVACY COMMITMENT AND PERSONAL INFORMATION

Capital One is committed to keeping personal information, accurate, confidential and secure.

We collect, use and disclose information to operate our business and as required by law. Personal information is information about an identifiable individual, as defined in the *Personal Information Protection and Electronic Documents Act*.

2. CHANGES TO PRIVACY POLICY

This Privacy Policy ("Policy") describes our current privacy practices. We update this Policy on an ongoing basis to ensure consumers, applicants and customers are aware of updates to our privacy practices, to streamline those practices and to comply with applicable laws. Consumers are individuals who are not currently our customers; applicants are individuals who apply to become our customers; and customers are individuals who have been approved, use or have used our products and services in the past. Please visit this site regularly for updates.

3. ACCOUNTABILITY

Our Privacy Officer is responsible for ensuring that we comply with this Policy and applicable laws. **We are responsible for personal information in our possession or custody, including personal information transferred to a third party for processing**. More details on our third parties are below under "Limiting Use, Disclosure and Retention".

4. IDENTIFYING PURPOSES

Capital One clearly identifies the purposes for which personal information is collected, used or disclosed prior to or at the time of collection.

Capital One may collect, use and disclose personal information of consumers, applicants and customers to develop, analyze and advertise products and services, process applications, maintain and service accounts, and comply with applicable laws.

Except where information is marked as mandatory, you get to decide what information you want to share with us.

Information We Collect

Consumers and applicants. **We may collect information about consumers who are not our current customers, so we can develop our products and services. Sometimes this information comes from lists like the telephone book or other public directories.**

When a consumer applies to be our customer, we may collect the information previously given by the consumer (such as name, address, telephone number and date of birth). **We may also use publicly available information for verification purposes; this may include, but is not limited to, financial and employment information obtained from business directories and government websites.**

We may also collect information from surveys that consumers and applicants participate in, or third parties that consumers and applicants engage with. We may collect information from consumers and applicants' mobile and online activity; for example, Internet Protocol (IP) address, mobile device ID, application and website use, and history. Cookies (small computer files that a website's server places on your computer) collect information about your online behaviour. You can set your browser to reject cookies, but this may impair your website visits and functionality.

Customers. When you become a customer, the information you provided to us as a consumer or an applicant may be transferred with your file. When you are a customer, we may collect and store information to help us verify the effectiveness of our products and services, to monitor your usage and to better tailor our services to your needs and interests. We may collect information about your transactions, including purchases, account balances, fees, payment history, parties to transactions and credit card usage. We may collect information from credit reporting agencies and other outside sources to verify financial information about you, such as your employment and credit history. If you give us your SIN, we may use it to identify you with credit reporting agencies and other parties; we may keep this information along with other information about you in our records, even after your account is closed. When you provide authorized user information, we expect that you have authority to consent to its collection, use, and disclosure as outlined in this Policy.

We may also collect information from surveys that customers participate in, or third parties that customers engage with. We may collect information from customers' mobile and online activity; for example, IP address, mobile device ID, application and website use, and history.

Communication. When you have a telephone conversation with one of our representatives, your call may be recorded for quality, training and record retention purposes. If purposes**. If you choose to contact us by email, we may retain your email address, the content of your communication and our response.**

Use of Information

We may use your information to contact you. **Your information allows us to contact you to respond to your questions, proactively notify you about your account where necessary, inform you about our products and services, and update you on changes to our website. We may use your information to send you important updates about your application status and account opening disclosures, and important messages about your account(s). When you communicate online or by email, you acknowledge that sending information over the Internet isn't secure, as it can be intercepted and/or manipulated and retransmitted.**

We may use your information to authenticate you. **With your information, we can confirm your identity, credit status and financial standing, and this information enables us to consider your application(s) for products and services.**

We may use your information to assess your creditworthiness. **With your information, we can assess your creditworthiness to determine your eligibility for products and services, and process your application(s). This information is helpful for us to offer you product choices that are suitable for you.**

We may use your information to service you. Your information may be used to maintain, service, process, analyze, audit and collect on your account(s). For example, loyalty reward numbers and program statuses are used to align your account with cobranded credit card loyalty rewards providers. We may also use your information to service your mobile account, provide you with a unique user experience, optimize our website and perform analytics. We may also send notifications and support mobile payments with this information. In addition, we may update and / or provide information regarding your credit card or account pursuant to the MasterCard Automatic Billing Updater as amended from time to time or pursuant to

other industry standards.

We also customize our website and mobile applications based on information collected, and use it to understand and deliver products and services that you, and others who are similar to you, may find useful. The information is used to better understand our website and mobile application activity, and how users interact with our digital sites. It's also used to monitor and improve our website and mobile applications.

We may use your information to make improvements. **We may use your personal information to evaluate existing products and services, develop new products and services, drive strategy and improve the customer experience we offer. Information we collect is also valuable for our quality and servicing training programs.**

We may use your information to prevent fraud. **We may use your information to assess fraud and other risks to you and Capital One, and to protect consumers, applicants and customers from identity theft, fraud and unauthorized account access. When investigating fraud, we may ask for identification documents (such as a Canadian driver's licence, Canadian passport, birth certificate, utility bill or bank statement, or other forms of identification).**

We may use your information to serve you offers, advertising and marketing. **Elements of your personal information may be used to determine your suitability, or to directly communicate with you, for targeted advertising, marketing, promotions, rewards programs, research or contests. You may see advertisements for our products and services on our website, mobile applications or on third-party websites, based on your online or mobile activity and information you've shared with third parties.**

We may use your personal information to identify you on third-party platforms you already use (such as Facebook and Twitter) and serve you ads through their marketing platforms. We may also use your information to identify you on third-party platforms (such as Facebook and Google), and then use the algorithms of those platforms to find other people with similar characteristics.

Where your credit score is used for the purposes of advertising, express opt-in consent will be captured from you at the time of collection.

We may prevent you from seeing Capital One offers that are unsuitable for you, based on the information you've provided to us.

We may use your information to report. We may share application and transaction information with consumer reporting agencies and other parties who have financial, employment or business dealings with you.

5. CONSENT

If you apply for a credit product, communicate with us or provide personal information to us in any way, you acknowledge your consent for personal information collection, use and disclosure as set out in this Policy or applicable laws and industry standards. If we want to use your information for a purpose that was not disclosed at the time of initial consent, consent will be sought at the time of this new purpose.

Updating consent. **You can withdraw your consent for use and disclosure of your personal information, other than that which is required for us to maintain and service your account, subject to legal and contractual restrictions, with reasonable notice to Capital One. You can also request that we don't contact you for advertising, marketing, promotions, rewards programs, research or contests; however, we may still need to contact you to comply with applicable laws or for business needs.**

To update your privacy preferences for specific accounts, please contact the following numbers:

[..]

Online Behavioural Advertising ("OBA"). We subscribe to the Digital Advertising Alliance of Canada's Self-Regulatory Principles for OBA. These principles promote consumers' awareness and choice about how their information is used for OBA. You can opt out of the use of your browsing habits for OBA – just visit the AdChoices website provided by the Digital Advertising Alliance of Canada, and use the opt-out mechanism. You can also click on the "AdChoices" link embedded in many of our ads to adjust your browser settings to reject cookies.

6. LIMITING COLLECTION

Capital One only collects personal information that's necessary for the purposes we identify, and as required by applicable laws.

7. LIMITING USE, DISCLOSURE AND RETENTION

Capital One limits use, disclosure and retention of personal information to the purposes we identify, and as required by applicable laws.

Third-party service providers. **We may share your personal information with service providers who perform services on our behalf (such as credit reporting, marketing, research, data processing and other services as required to service you). Our contracts with third parties include obligations to protect your personal information, and third parties must meet our rigorous privacy standards. When you engage with other companies directly, or contact us through their platforms, their use of the information they collect from you is subject to the terms of their privacy policies**.

Capital One Mastercard for Costco members.

[…]

SaksFirst Credit cardholders.

[…]

Hudson's Bay Mastercard and Hudson's Bay Credit Card customers.

[…]

Assignees. **We may, at any time, sell, transfer or assign any or all of our rights to our Canadian business, including our interests, rights or obligations regarding your account(s) with us. If we do so, we may share your personal information with prospective purchasers, transferees or assignees.**

Information processed outside Canada. **Your personal information may be stored and processed at our corporate offices in the U.S. or with approved third parties within the U.S. or elsewhere.**

If a third party processes or stores information outside Canada, foreign governments, courts or regulatory agencies may therefore be able to obtain such personal information through the laws of the foreign jurisdiction.

8. ACCURACY

Capital One ensures personal information is as accurate, complete and up to date as is necessary for

the purposes for which it is to be used.

If you believe that the personal information we have about you isn't accurate or complete, please contact us by using any of the methods noted in this Policy so we can update your personal information.

9. SAFEGUARDS

Capital One uses procedures and practices appropriate to the sensitivity of personal information to protect against loss, theft and unauthorized access. Access to your information is restricted to those individuals and parties who require access.

For example, we have physical security (such as restricted access to our offices and secure storage), electronic protection (such as passwords and encryption) and safe business practices (such as customer authentication when you call us). We also train our staff on how to safeguard personal information.

You can help us safeguard your information too. If you contact us through email or social media, you should avoid sending highly sensitive information, such as your banking information or full credit card number. We also recommend that you use unique and strong passwords for your online account(s) and that you don't share your passwords with anyone.

10. OPENNESS, INDIVIDUAL ACCESS AND CHALLENGING COMPLIANCE

You can write to our Privacy Office to request access to the personal information we have on file for you. We will provide you with the personal information we have, subject to certain considerations specified by law.

[…]

[70] As revealed by Capital One's Credit Card Agreement found in the Document Brief, Capital One's Application for Credit form stated:

APPLICATION FORM

[…]

FIRST NAME:
LAST NAME:
EMAIL:
STREET ADDRESS:
PHONE NUMBER:
DATE OF BIRTH:
SOCIAL INSURANCE NUMBER:
PLEASE CHECK ONE OF THE BOXES BELOW TO INDICATE YOUR EMPLOYMENT STATUS
( ) EMPLOYED ( ) UNEMPLOYED ( ) SELF-EMPLOYED ( ) RETIRED
EMPLOYER NAME:
ANNUAL PERSONAL INCOME:

[…]

MEMBERSHIP BILLING & APPLICATION SIGNATURE

[…]

APPLICATION SIGNATURE: By signing below, you certify that you have read and agree to the important Disclosures, Terms and Conditions of Privacy Statement, and that you have the

consent of any Authorized User designated on this application to the collection, use and disclosure or his/her personal information as set out in the Privacy Statement.

You acknowledge that your consent to the Privacy Statement includes the ability of Capital One Bank (Canada Branch), its affiliates or service vendors (on its behalf) to share and exchange credit reports or other information about you with credit reporting agencies, credit bureaus and others, from time to time, for the purpose of determining creditworthiness and verifying your identity

[…]

TERMS AND CONDITIONS

[…]

YOUR PRIVACY

We respect your privacy. Not only do we respect it, but we also protect it. We collect and provide your information as required for the standard operation of our business and as required by law. We may also release your information to companies that you have authorized us to release your information to, including service providers, credit reporting agencies, our affiliates and co-branding partners. These companies must first meet our rigorous privacy standards before we partner with them to do business with you.

[…]

CONFIDENTIALITY AND SECURITY

We have physical security, electronic protection and safe business practices to prevent identity theft. We restrict access to you personal information to those who need to have it to provide provide products or services to you, including service provide who provide services for use such as marketing, advertising and credit card embossing. We require those companies to keep the information we share with them safe and secure and we do not allow them to use or share information for any purpose other than the job they are hired to do.

INFORMATION WE COLLECT

Consumers **We may collect information about customers who are not our current customers, so we can develop our products and services. Sometimes this information comes from lists like the telephone book or other public directories.**

When a consumer applies to be our customer, we collect the information given during the application process (such as the consumer's name, address, telephone number and date of birth). We may also use publicly available information (such as financial and employment information obtained from business directories and government websites) for verification purposes when making credit decisions on an application.

Customers. **When you are a customer, we collect and store information to help us verify the effectiveness of our products and services to monitor your usage and to better tailor our services to your needs and interests. We collect information about your Transactions, including Purchases, Account balances, fees, payment history, parties to Transactions and credit card usage. We may collect information from credit reporting agencies and outside sources to verify financial** information about you, such as your employment and credit history.

Communication. […]

Website Visits. When you, as a consumer or our customer, visit our website or use our mobile application, we may collect certain information including your internet Protocol ("IP")

address and operating system, the date and time of your visit and information about the pages you visit while on our website. We may use electronic technologies such as cookies to help us understand what parts of our products and services you find most useful. You can reject cookies but the functionality of the website may be impaired and the efficiency of you web visit may be impacted.

USE OF INFORMATION

We want you to understand why we collect and use information about you and how this can benefit you. We collect and use information about consumers and customers so we or our service vendors (whether engaged by or on behalf of us or any of our assignees) can use it in the following ways:

> **(i) to open, maintain, service, process, analyze, survey, audit and collect on your account;**
>
> **(ii) to verify your identity and credit worthiness;**
>
> **(iii) to protect you from identity theft, fraud and unauthorized access to your account;**
>
> **(iv) to share application and transaction information with consumer reporting agencies and other parties who have financial, employment or business dealings with you and;**
>
> **(v) to determine your eligibility, administer and contact you for the purposes of marketing, promotions, rewards programs, research or contests; and**
>
> **(vi) to use for any purpose required by law.**

[…]

[71] As set out in the Document Brief, Capital One's credit card agreement stated:

Customer Agreement

We're happy to open your credit card account. This Agreement contains information about your account. Please read it and keep it for your records. In this Agreement, the words "you," "your" and "yours" refer to the applicant and any co-applicant who, according to our records, was identified as such as part of the application, meaning the request to us for the account. These words do not include an authorized user. The words "we," "us" and "our" mean the Capital One® Bank (Canada Branch) and its successors or assigns. The word "transaction" means purchases, cash advances, special transfers, balance transfers, Account Access Cheque use, credits, mail or phone orders, or any other use of the account. The terms of our Privacy Statement are incorporated as part of the terms of this Agreement.

[…]

Privacy Statement

Our Commitment to Protecting Your Privacy

Capital One® is committed to keeping your personal information accurate, confidential and secure. We want to earn your trust by providing strict safeguards to protect your information.

What is Personal Information?

Personal information is any information that can identify you.

Your Privacy

We respect your privacy. Not only do we respect it, but we also protect it. The personal information you share with us, stays with us.

We collect and provide your information as required for the standard operation of our business and as required by law. We may also release your information to companies that you have authorized us to release your information to, including service providers (such as the printers of our account statements), credit reporting agencies (like TransUnion and Equifax), our own affiliates and co-branding partners for co-branded rewards card. These companies must first meet our rigorous privacy standards before we partner with them to do business for you.

[…]

Access to Personal Information About You

You may request access to the personal information we collect about you. We will answer your inquiry and/or provide you with access to this information, subject to certain considerations specified by law. To request access to your personal information in our possession, write to us at Attention: […]

Confidentiality and Security

We have physical security (access in buildings), electronic protection (encryption), and safe business practices (customer authentication when you call us) to prevent identity theft. We restrict access to your personal information to those who need to have it to provide products or services to you. We use other companies to provide services for us such as marketing, advertising and credit card embossing, but select these companies carefully and require them to keep the information we share with them safe and secure. We do not allow them to use or share information for any purpose other than the job they are hired to do.

[…]

Information We Collect

Consumers. We may collect information about consumers who are not our current customers, so we can develop our products and services. Sometimes this information comes from lists like the telephone book. When a consumer applies to be our customer, we collect the information given during the application process (such as the consumer's name, address, telephone number and date of birth).

Customers. When you are a customer, we collect and store information to help us verify the effectiveness of our products and services, to monitor your usage and to better tailor our services to your needs and interests. We collect information about your transactions, including purchases, account balances, fees, payment history, parties to transactions, and credit card usage. We may collect information from credit reporting agencies and other outside sources to verify financial information about you, such as your employment and credit history.

Website visits. When you visit our Web site, we may collect information about your use of our products and services, which is captured in a common log file format, including your Internet Protocol ("IP") address and operating system, the date and time of your visit and information about the pages you visit while on our Web site. To assist us in collecting information when you visit us online, we may use electronic technologies such as cookies (small computer files saved to your computer's hard drive) which help us understand what parts of our products and services you find most useful. You can reject cookies, but sometimes this compromises the functionality of the product or service.

Use of Information

We want you to understand why we collect and use information about you and how this can benefit you. By knowing more about our customers, we and our business partners can provide specialized products that may be of interest to you and your family. We collect and use information about consumers and customers so we or our service vendors (whether engaged by or on behalf of us or any of our assignees) can use it in the following ways:

(i) to open, maintain, service, process, analyze, survey, audit and collect on your account;

(ii) to verify your identity and credit worthiness;

(iii) to protect you from identity theft, fraud and unauthorized access to your account;

(iv) to share application and transaction information with consumer reporting agencies and other parties who have financial, employment or business dealings with you and;

(v) to determine your eligibility, administer and contact you for the purposes of marketing, promotions, rewards programs, research or contests; and

(vi) to use for any purpose required by law.

This information may also be shared with any person or entity to which we have assigned or transferred an interest in your account, any debt or interest due or any of our rights or obligations under any agreement with you (including any subsequent assignee).

We may also use your information to respond to your questions or to contact you in order to notify you of functional changes to our Web site or to our products and services. If you choose to contact us, we may retain your e-mail address, the content of your communication and our response.

We may contact you by e-mail using the e-mail address you provided for special offers or standard service messages. To ensure your security, we will not include sensitive information in an e-mail such as your full 16-digit account number, date of birth, social insurance number (if provided) or account balance.

In the event that a service vendor is located outside of Canada, the information on file for you or an authorized user (as set out below) may be processed and stored outside Canada and foreign governments, courts of law enforcement or regulatory agencies may be able to obtain disclosure of this information. We may, at any time, sell, transfer or assign any or all of our rights to our Canadian business including your account and if we do so, we may share information concerning you and any authorized user with prospective purchasers, transferees or assignees.

In the event that a service vendor is located in the United States, the information on file for you or an authorized be processed and stored in the United States and the United States governments, courts of law enforcement or regulatory agencies may be able to obtain disclosure of this information through the laws of the United States. We may, at any time, sell, transfer or assign any or all of our rights under this Agreement and if we do so, we may share information concerning you and any authorized user with prospective purchasers, transferees or assignees.

Sharing of Information

Service vendors and credit reporting agencies. We may share information with our service vendors (statement printing), service providers (MasterCard® International) and credit

reporting agencies (TransUnion and Equifax) for the purposes described above in Use of Information. Assignees. We may, at any time, sell, transfer or assign any or all of our interests, rights or obligations with respect to your account with us. If we do so, we can share your personal information with prospective purchasers, transferees or assignees.

Other third parties. **We may share with carefully selected business partners information we collect about our customers, former customers, and withdrawn or declined applicants, such as name, street address, e-mail address and telephone number, for the purpose of determining the eligibility of customers and consumers for valuable products and services (such as credit balance insurance and credit report monitoring) offered by us or our business partners. We may share customer information with other parties who have financial, employment or business dealings with you. If you give us your Social Insurance Number, we may use it to identify you with credit reporting agencies and other parties, and we may keep it along with other information about you in our records, even after your account is closed to use for the purposes stated above. We ensure that any third party is bound to respect your privacy rights in the same way that we are.**

[…]

Your Consent

If you apply for credit, or by communicating or providing information to us in any other way, you acknowledge your consent for personal information collection, protection, use, disclosure and retention as set out herein. Subject to legal and contractual restrictions, you may withdraw your consent at any time after your account has been opened with reasonable notice. If at some point we want to use your personal information for any purpose other than the ones specified, we will inform you before using the information for this new purpose. We may inform you by posting a notice to our Web site or by communicating with you directly.

[…]

F. Material Facts

[72] The Plaintiffs' Fresh as Amended Statement of Claim is set out in the annexed Schedule "A."

[73] In this section of my Reasons for Decision, first, I shall extract the material and other facts from the Fresh as Amended Statement of Claim that are needed for the purposes of Phase I of the Certification motion. I shall be generous and liberal in the extraction and include some facts that are more evidentiary than material facts. Second, I shall compare and contrast the data breach case that could have been pleaded with the data misappropriation and misuse case that is found in the Fresh as Amended Statement of Claim.

1. The Material and Other Facts as Pleaded in the Fresh as Amended Statement of Claim

[74] The material and other facts from the Fresh as Amended Statement of Claim are as follows.

[75] The Class is comprised of persons in Canada who applied for Capital One credit cards between 2005 and 2019 and/or provided confidential financial and personal information to Capital One or contracting parties contracting with Capital One in Canada, including the Bay, Costco, WalMart, JC Penney and MasterCard. Capital One collected the applicants' Social Insurance Number ("SIN"), their bank account numbers, credit history, names, addresses, and dates of birth

for the singular purpose of assessing credit worthiness and eligibility for a credit card. The data was stored on Capital One's computer servers.

[76] Capital One Financial Corporation is the parent of United States subsidiaries, Capital One, N.A., and Capital One Bank (USA), N.A. and of Canadian subsidiaries Capital One Bank (Canada Branch) and Capital One (Services) Canada Inc. From January 1, 2005 to July 30, 2019 (the Class Period), approximately six million Canadians applied for credit cards and provided Capital One with confidential personal information. The Plaintiff Rina Del Giudice, who resides in Ontario, and the Plaintiff Daniel Wood, who resides in Alberta, are Capital One card holders.

[77] Capital One and its American subsidiaries began its modern business in 1994 as a regional financial institution with aspirations to be a bank. Its business focused on consumer credit including credit cards. Between 1994 and 2005, Capital One surpassed its competitors and became the industry leader in the financial credit industry. Responding to the advancements in technology that would transform the economy, Capital One developed an innovative information-based strategy that transformed the credit industry. Capital One developed customized or tailored credit cards. Capital One obtained personal data from applicants for credit and appropriated it, merchandized it, and monetized it to earn revenue and to grow its business. Capital One profited from the internal and external use of the personal information obtained from applicants for its credit cards.

[78] Around 2005, Capital One was approved to become a bank by the Unites States' Federal Reserve Board. Capital One then aspired to expand and to operate in international markets. Capital One targeted Canada as a new market for its goods and services and as a source of more data and personal information.

[79] The Plaintiffs plead that with its achievement of its goal of becoming a bank holding company, Capital One assumed trust and fiduciary obligations to its customers and to those applying to be credit card holders. The Plaintiffs plead that the information from the applicants was held by Capital One for a single purpose use. The Plaintiffs plead that the use of the information for any other purpose was a breach of trust and fiduciary duty owed to the applicants for credit cards.

[80] Having developed its plans between 2005 and 2015, Capital One implemented its Canada Campaign to expand its business into Canada. To this end, it incorporated subsidiaries Capital One Bank (Canada Branch), which was incorporated under the federal *Bank Act* in 2005, and Capital One (Services) Canada Inc. Capital One adopted the same business model for Canada, including using, merchandizing, and monetizing applicant information. Capital One's goals in Canada were twofold: first, to market its credit cards; and second, to mine and merchandize the data.

[81] The Plaintiffs plead that Capital One Bank (Canada Branch) was bound to observe the laws of Canada including *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[32] and other laws that regulate the obtaining and the use that can be made of personal information. The Plaintiffs allege that the business model used in Canada did not comply with banking, privacy, and consumer protection laws and regulations.

[82] The Plaintiffs plead that in breach of trust and fiduciary duty, Capital One used the Canadian applicants' personal information. The Plaintiffs plead that the use of the information for any other purpose other than applying for credit was a breach of trust and fiduciary duty owed to

[32] SC 2000, c. 5.

the applicants for credit cards. The Plaintiffs plead that the use of the information for any other purpose was unlawful unless a meaningful consent was obtained under PIPEDA, which did not occur.

[83] The Plaintiffs allege that Capital One's retention of the data after its single use was finished exposed the applicants to risk that their data could be obtained by and improperly used by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties.

[84] The Plaintiffs allege that knowing of the rapid changes in information technology, Capital One knew that by retaining and using the personal information of its card applicants, there was an ever-increasing risk of a data breach that would expose applicants to having the data misused by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties. The Plaintiffs plead that because of the exponential growth in information technology, each day that passed of improper retention increased the risk of a data breach.

[85] The Plaintiffs plead that Capital One knowingly, intentionally, and recklessly failed to give regular and meaningful notice to the applicants for credit cards of the retention, migration, storage, and internal and external use of the confidential data by Capital One and of the increasing risk the data would be obtained by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties. The Plaintiffs plead that a data breach was inevitable.

[86] The Plaintiffs allege that around 2015, when financial businesses were under increasing competitive pressures to cut costs and increase profit margins, the personal data obtained in Canada was delivered (migrated) outside of Canada to Capital One's computer servers in the United States and to Amazon Web storage facilities. The Plaintiffs allege that this migration of data was unauthorized and unlawful. The Plaintiffs allege that the migration of the data to the U.S. was an intentional breach of data protection laws and of banking trust obligations.

[87] With respect to the storage of personal information, the Plaintiffs plead that Capital One contracted to use Amazon Web, which operates a cloud-based data storage system. Amazon Web operates global data centres for storing computer data from third party enterprises including Capital One. The Plaintiffs plead that it was known to Amazon Web and Capital One or it ought to have been known by them that Amazon Web's firewall was misconfigured or could be misconfigured by permissions set by Capital One making the stored data vulnerable. The Plaintiffs allege that the failure to repair the flaws in the computer systems of Capital One and of Amazon Web was a breach of a duty of care to the applicants for Capital One's credit cards. The Plaintiffs plead that Amazon Web could have and should have deployed computer protection services to ameliorate the flaws in the storage infrastructures. The Plaintiffs plead that Capital One and Amazon Web failed to regularly test its security measures and to repair deficiencies and to protect and manage risks of data breach and cyber-attacks.

[88] The Plaintiffs plead that the Defendants' conduct increased further the risk of harm to the Class Members. The Plaintiffs plead that the Defendants' carelessness constituted intentional and reckless actions and unconscionably contributed to the increased risk of a data breach by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties.

[89] The Plaintiffs plead that Capital One and Amazon Web breached their duty of care and a duty to warn. The Plaintiffs plead that the conduct of Capital One and Amazon Web was highly offensive to any reasonable person and caused the class members and the Plaintiffs damage in the form of increased risk of loss of privacy. The Plaintiffs plead that Capital One and Amazon Web failed to protect the class members' rights under s. 8 of the *Canadian Charter of Rights and Freedoms*[33],and failed to live up to the reasonable expectations that they would protect the privacy of each and every Class Member.

[90] The Plaintiffs plead that Amazon Web was obliged to ensure that it was receiving data that was owned by Capital One but failed to do so. The Plaintiffs plead that by accepting the data Amazon Web assumed all of Capital One's duties of care, duties to warn, and legal obligations to protect the data including complying with data protection and privacy laws and banking trust obligations.

[91] The Plaintiffs plead that the risk of data breach was increased when Capital One aggregated the Canadian data with the American data creating a data base of 100 million persons. The Plaintiffs plead that the aggregation of all the confidential data presented an attractive target for data abusers thereby exponentially increasing the risk of a data breach. The Plaintiffs plead that the migration of the data to Amazon Web increased the risk of a data breach and the misuse of the personal information by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties.

[92] The Plaintiffs plead that the aggregation of the data was an intentional and/or wholly reckless unauthorized retention, use of and risk to confidential data in breach of Capital One's obligations to protect the privacy and safety of the confidential data.

[93] The Plaintiffs plead given the exponentially increased risks that the migration of the data to Amazon Web would expose the data to data abusers and given that the decision to do so was motivated by the executives' purpose of enhancing their own wealth, the resulting increased corporate and individual profits was highly offensive to any reasonable person, giving rise to intentional and/or reckless conduct for liability, damages, moral damages, punitive and aggravated damages and an order of aggregated damages under the relevant Class Proceedings Acts for the intentional conduct.

[94] The Plaintiffs plead that the conduct of Capital One and Amazon Web was highly offensive to any reasonable person and caused the Class Members damage in the form of increased risk and ultimately their loss of privacy.

[95] Pausing here in the recitation of the material facts, it may be observed that the predominant narrative concerns the alleged misappropriation and misuse of the Class Members' personal information and the potentiality of a breach of privacy. It is only late in the Fresh as Amended Statement of Claim, paragraph 86 of the 134-paragraph pleading, that the Plaintiffs address the role of the defendant Paige A. Thompson and the material facts of the data breach that precipitated the Plaintiffs' proposed class action.

[96] Ms. Thompson is a computer systems engineer residing in the U.S. Her internet name was "ERRATIC." Ms. Thompson was an employee of Amazon Web between 2016 and 2018. The Plaintiffs allege that Amazon Web had a duty to supervise Ms. Thompson after she left their employment. The Plaintiffs also allege that Ms. Thompson was an employee of Capital One given

[33] R.S.C. 1985, App. II, No. 44, Schedule B.

its contractual relationship with Amazon Web.

[97] The Plaintiffs plead that beginning around March 12, 2019, and continuing into April 2019, knowing of the defects in Amazon Web's infrastructure, Ms. Thompson pierced the firewall and exfiltrated the Class Members' confidential personal information, including SINs, names, addresses, dates of birth, bank account numbers and credit history.

[98] The Plaintiffs plead that the SINs were encrypted or tokenized, but Ms. Thompson and others decrypted the code making the SINs available to any person with access to the internet including organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments.

[99] Ms. Thompson posted the confidential data on GitHub, Inc., which is an American corporation that operates a website for software developers and information technology experts. The Plaintiffs plead that the data became available to organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments causing existing and ongoing damage to Class Members.

[100] The Plaintiffs plead that Capital One and Amazon Web failed to discover the exfiltration of the confidential data by Thompson and its being published to the world on GitHub.

[101] In June 2019, Thompson and others reported the data breach to the world. The Plaintiffs plead that Capital One and Amazon Web failed to discover the infiltration, exfiltration and publication of the confidential data for almost three months, from April 21, 2019 to July 17, 2019.

[102] The Plaintiffs plead that because of lack of supervision of Ms. Thompson during and after her employment at Amazon Web, Capital One and Amazon Web fell below the data protection laws and failed in their duty of care owed to the Class Members and are liable for all damages flowing from the data breach and the improper publication of the confidential data. The Plaintiffs plead that Capital One, Amazon Web, and GitHub are vicariously liable for Thompson's breach of confidence, breach of trust, breach of privacy, intentional and/or reckless intrusion upon seclusion, misappropriation of the identity and conversion of the confidential data.

[103] The Plaintiffs plead that Capital One and Amazon Web owed a duty to warn the Class Members and that they breached this duty. The Plaintiffs plead that the notice given on July 29, 2019 was a late and an inadequate warning to the six million Canadians whose confidential data had been published through the Internet to organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments. The Plaintiffs plead Capital One and Amazon Web owed a duty to warn the Class Members of the ever-increasing risks of the data breach when it occurred, and the publication of the confidential data on the World Wide Web.

[104] As an alternative to the other causes of action, the Plaintiffs plead that if a contract existed between Capital One and any of the Class Members, Capital One was in breach of contract and in negligent breach of contract in maintaining, storing and using the confidential data after the single purpose use was spent.

[105] The Plaintiffs plead that Ms. Thompson, Capital One, and Amazon Web are liable for general damages, punitive damages, exemplary damages, aggravated damages, aggregated damages pursuant to the Class Proceedings Acts and damages for causing and threatening to cause distress, humiliation, anguish, damages, and moral damages; namely: (i) threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; (ii) loss of confidence in

the banking and financial system; (iii) identity theft, crime, fraud and abuse, resulting in monetary loss and economic harm; (iv) loss of the value of privacy and the confidentiality of the stolen confidential data; (v) the illegal sale of the compromised data on the deep web black market; (vi) expenses and/or time spent on credit monitoring and identity theft insurance; (vii) time spent scrutinizing bank statements, credit card statements, and credit reports; (viii) expenses and/or time spent initiating fraud alerts; and (ix) decreased credit scores and ratings; (x) damages arising from distress, humiliation, anguish arising from the highly offensive acts of Capital One in converting the Class Plaintiffs' Confidential Data to Capital One's own use for profit and recklessly and intentionally exposing the Confidential Data to publication to the world, including Data Abusers by reason of the wrongful conduct, negligence and breaches described above.

[106] The Plaintiffs plead that the Class Plaintiffs are entitled to an award of aggregate damages amounting to $20,000 per Class Plaintiff [$120 billion in the aggregate] pursuant to the relevant Class Proceedings Acts.

[107] The Plaintiffs plead that the Class Plaintiffs are entitled to exemplary and punitive damages in the amount of $100-million and moral and aggravated damages in the amount of $20,000 per Class Plaintiff [$120 billion in the aggregate].

[108] Pausing here, it is interesting to note that at the time of the carriage motion, the claim was for damages in the amount of $1,500 per person impacted in Canada solely by the breach of Personal Information excluding their SIN; and $2,500 (an additional $1,900) per person for those whose SIN was included in the breach, based upon the breach of Personal Information of a total of six million Canadians, including the SIN of one million Canadians [$10.9 billion]. At the time of the carriage motion, the claim was for $15 million for special damages and $25 million for punitive damages.

[109] In addition, the Plaintiffs plead that the Class Plaintiffs are entitled to an accounting for profits made by Capital One and Amazon Web from the sale, use, fees and interest charges from the use of credit cards during the Class Period for each Class Member and an Order that the profits be disgorged in favour of the Class Members in addition to the types of damage set out above.

2. The Contrasting Factual Narratives

[110] For the discussion that follows in these Reasons for Decision, it is helpful to summarize and to compare and contrast the data breach case that could have been pleaded with the data misappropriation and misuse case that is found in the Fresh as Amended Statement of Claim.

[111] The factual narrative of the Plaintiffs' data misappropriation and misuse case extends from 1994 to 2019 (26 years). It is a longer narrative than the 2005 to 2019 period (15 years) of a data breach case.

[112] The narrative of the Fresh as Amended Statement of Claim is a longer and more intricate narrative than the data breach case because the narrative of the data misappropriation and misuse case makes events that are just background and minor facts in the data breach case, major foreground facts for the data misappropriation and misuse case. The factual narrative of the data misappropriation and misuse case is intense, intricate, complex, and sophisticated in contrast to the more straightforward and rudimentary narrative of the data breach case.

[113] The narrative of a data breach case is that in 2015, Capital One expanded its banking business into Canada where six million Canadians applied for Capital One credit cards. Capital

One promised to keep the personal information provided by the applicants for its credit cards private and confidential. Capital One hired Amazon Web to store the personal information on its servers. It is alleged that Capital One and Amazon Web were negligent in how the personal information data was stored. In March 2019, Ms. Thompson, a former employee of Amazon Web hacked the Amazon Web computer servers and then posted the extracted confidential information of the six million Canadians on the GitHub website. The data breach was not discovered for four months, and in July 2019, Capital One advised the six million Canadians that their personal information had been posted on the Internet for the whole world to see.

[114] The narrative of the data misappropriation and misuse case is that Capital One commenced business in 1994 as a regional financial business that by 2005 had grown into a bank with international aspirations, which brought it to Canada in 2005. Capital One's business model was to use advances in computer technology to commercialize the personal information it collected from its customers and from those who would be its customers. Using the rapidly accelerating developments in computer technology, there was big money to be made in marketing the big data of personal information. Capital One became a very successful and profitable miner of personal information which was a revenue-producing business asset. However, in collecting personal information, there was also ever-increasing risks to the protection of the privacy of the personal information, because the aggregation of big data attracts the interest of organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties who could profit from the misappropriation and misuse of the personal data. Despite these risks, Capital One expanded its business, and when Capital One came to Canada, it came as a bank and it assumed fiduciary responsibilities commensurate with the risks. When Capital One came to Canada, it agreed to be bound by the statutory and common law provisions that govern the collection, retention, and protection of personal information. In Canada, six million Canadians completed application forms to obtain Capital One credit cards. In applying for credit cards, the six million Canadians each provided personal information. Capital One collected the personal information for the single purpose of determining whether to agree to enter into a credit card agreement with the applicant. In violation of its obligation to use the data it collected for this single use, Capital One did not return and rather kept the six million Canadians' personal information data. Capital One aggregated the personal information into big data to enhance its business and to make money from the personal information. Unknown to the six million Canadian applicants, Capital One had retained Amazon Web to store the collected personal information on its servers in the United States. On the Amazon Web servers, the personal information of the Canadians was aggregated with the personal information of one hundred million American consumers. It is alleged that Capital One and Amazon Web were negligent in how the personal information data was stored. The Amazon Web storage facilities were negligently designed, configured, and administered making them inevitably vulnerable to computer hacking. The aggregation of the Canadian data with the American data and the migration of the Canadian data to the United States further increased the risk of the data being misused by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties. A data breach was inevitable and did in fact occur when in March 2019, Ms. Thompson, a former employee of Amazon Web, hacked its computer servers and posted the confidential information of the six million Canadians on the GitHub website. The data breach was not discovered for four months, and in July 2019, Capital One advised the six million Canadians that their personal information had been posted on the Internet for the whole world to see.

G. The Cause of Action Criterion:

1. The Pleaded Causes of Action

[115] In the Fresh as Amended Statement of Claim, the Plaintiffs allege the following nineteen causes of action; (a) appropriation of the name and information of the Class Plaintiffs [*i.e.*, "Class Members"] for the advantage of Capital One; (b) breach of confidence; (c) breach of duty to warn; (d) breach of fiduciary duty; (e) breach of privacy; (f) breach of ten statutes;[34] (g) breach of trust; (h) intentional and/or reckless conduct leading to intrusion upon seclusion; (i) negligence, and (j) negligent breach of contract.

[116] The pleaded causes of action against Paige Thompson are: (a) conversion; (b) intentional intrusion upon seclusion; (c) reckless intrusion upon seclusion; (d) intentional misappropriation of Financial Personality; (e) reckless misappropriation of Financial Personality, (f) breach of a duty to warn; (g) negligence and (h) breach of contract and negligent breach of contract.

[117] The pleaded causes of action against Capital One are: (a) conversion; (b) intentional intrusion upon seclusion; (c) reckless intrusion upon seclusion; (d) intentional misappropriation of Financial Personality; (e) reckless misappropriation of Financial Personality, (f) breach of data protection laws; (g) breach of a duty to warn; (h) breach of confidence, trust, and fiduciary duty; (i) negligence; (j) strict liability; and (k) breach of contract and negligent breach of contract.

[118] The pleaded causes of action against Amazon Web are: (a) conversion; (b) intentional intrusion upon seclusion; (c) reckless intrusion upon seclusion; (d) intentional misappropriation of Financial Personality; (e) reckless misappropriation of Financial Personality, (f) breach of data protection laws; (g) breach of a duty to warn; (h) negligence; (i) strict liability; and (j) breach of contract and negligent breach of contract.

2. General Principles: the Cause of Action Criterion

[119] In this section of my Reasons for Decision, I set out the general principles for the cause of action criterion.

[120] The first criterion for certification is that the plaintiff's pleading discloses a cause of action. The "plain and obvious" test from Rule 21 of the *Rules of Civil Procedure* for disclosing a cause of action from *Hunt v. Carey Canada*,[35] is used to determine whether a proposed class proceeding discloses a cause of action for the purposes of s. 5(1)(a) of the *Class Proceedings Act, 1992*. To satisfy the first criterion for certification, a claim will be satisfactory, unless it has a radical defect, or it is plain and obvious that it could not succeed.[36]

---

[34] The ten statutes alleged to have been breached are: (a) *Consumer Protection Act, 2002,* S.O. 2002, c. 30, Schedule A; (b) *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40; (c) *Electronic Commerce Act*, 2000, S.O. 2000, c. 17; (d) *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; (e) *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; (f) *Privacy Act*, R.S.B.C. 1996, c. 373; (g) *Privacy Act*, RSC 1985, c P-21; (h) *The Privacy Act*, C.C.S.M., c. P125; (i) *Privacy Act*, R.S.N.L. 1990, c. P-22; and (j) *The Privacy Act*, R.S.S. 1978, c. P-24.

[35] [1990] 2 S.C.R. 959.

[36] *176560 Ontario Ltd. v. Great Atlantic & Pacific Co. of Canada Ltd.* (2002), 62 O.R. (3d) 535 at para. 19 (S.C.J.), leave to appeal granted, 64 O.R. (3d) 42 (S.C.J.), aff'd (2004), 70 O.R. (3d) 182 (Div. Ct.); *Anderson v. Wilson* (1999), 44 O.R. (3d) 673 at p. 679 (C.A.), leave to appeal to S.C.C. ref'd, [1999] S.C.C.A. No. 476.

[121] The failure to establish a cause of action usually arises in one of two ways: (1) the allegations in the statement of claim do not plead all the elements necessary for a recognized cause of action; or (2) the allegations in the statement of claim do not come within a recognized cause of action.[37]

[122] Matters of law that are not fully settled should not be disposed of on a motion to strike an action for not disclosing a reasonable cause of action,[38] and the court's power to strike a claim is exercised only in the clearest cases.[39] The law must be allowed to evolve, and the novelty of a claim will not militate against a plaintiff.[40] However, a novel claim must have some elements of a cause of action recognized in law and be a reasonably logical and arguable extension of established law.[41]

[123] In *R. v. Imperial Tobacco Canada Ltd.*,[42] the Supreme Court of Canada noted that although the tool of a motion to strike for failure to disclose a reasonable cause of action must be used with considerable care, it is a valuable tool because it promotes judicial efficiency by removing claims that have no reasonable prospect of success and it promotes correct results by allowing judges to focus their attention on claims with a reasonable chance of success.

[124] In *Atlantic Lottery Corp. Inc. v. Babstock*,[43] the Supreme Court stated that the test applicable on a motion to strike is a high standard that calls on courts to read the claim as generously as possible because cases should, if possible, be disposed of on their merits based on the concrete evidence presented before judges at trial. That said, in *Atlantic Lottery Corp. Inc. v. Babstock*,[44] in order to promote timely and affordable access to justice, the Supreme Court encouraged lower courts where possible to resolve legal disputes promptly rather than referring them to a full trial.

[125] Documents referred to in a pleading are incorporated by reference into the pleading, and on a motion to determine whether the plaintiff has plead a legally viable cause of action, the court is entitled to consider any documents specifically referred to and relied on in a pleading.[45]

[126] On a pleadings motion, the court accepts the pleaded allegations of material fact as proven,

---

[37] *2106701 Ontario Inc. (c.o.b. Novajet) v. 2288450 Ontario Ltd.*, 2016 ONSC 2673 at para. 42; *Aristocrat Restaurants Ltd. v. Ontario*, [2004] O.J. No. 5164 (S.C.J.); *Dawson v. Rexcraft Storage & Warehouse Inc.*, [1998] O.J. No. 3240 at para. 10 (C.A.).
[38] *Dawson v. Rexcraft Storage & Warehouse Inc.* (1998), 164 D.L.R. (4th) 257 (Ont. C.A.).
[39] *Temelini v. Ontario Provincial Police (Commissioner)* (1990), 73 O.R. (2d) 664 (C.A.).
[40] *Johnson v. Adamson* (1981), 34 O.R. (2d) 236 (C.A.), leave to appeal to the S.C.C. refused (1982), 35 O.R. (2d) 64n.
[41] *Silver v. Imax Corp.*, [2009] O.J. No. 5585 (S.C.J.) at para. 20; *Silver v. DDJ Canadian High Yield Fund*, [2006] O.J. No. 2503 (S.C.J.).
[42] 2011 SCC 42 at paras. 17-25.
[43] 2020 SCC 19 at para. 87–88.
[44] 2020 SCC 19 at para. 18.
[45] *Jordan v. CIBC Mortgages Inc.*, 2019 ONSC 1178 at paras. 72, 115; *Das v. George Weston Limited*, 2018 ONCA 1053 at paras. 31, 71, 74 and 78; *Kalra v. Mercedes Benz Canada Inc.*, 2017 ONSC 3795 at para. 24; *McCreight v. Canada (Attorney General)*, 2013 ONCA 483 at para. 32; *Tender Choice Foods Inc. v. Versacold Logistics Canada Inc.*, 2013 ONSC 80 at para. 31, aff'd 2013 ONCA 474; *Weninger Farms Ltd. v. Canada (Minister of National Revenue)*, 2012 ONSC 4544 at paras. 11-12; *Martin v. Astrazeneca Pharmaceuticals PLC*, 2012 ONSC 2744 at paras. 160-162, aff'd 2013 ONSC 1169 (Div. Ct.); *Re*Collections Inc. v. Toronto-Dominion Bank*, 2010 ONSC 6560; *Web Offset Publications Ltd. v. Vickery* (1999), 43 O.R. (3d) 802 (C.A.), leave to appeal dismissed, [1999] SCCA No. 460; *Corktown Films Inc. v. Ontario*, [1996] O.J. No. 3886 (Gen. Div.); *Montreal Trust Co. of Canada v. Toronto-Dominion Bank*, [1992] O.J. No. 1274 (Gen. Div.).

unless they are patently ridiculous or incapable of proof.[46] Bare allegations and conclusory legal statements based on assumption or speculation are not material facts; they are incapable of proof and, therefore, they are not assumed to be true for the purposes of a pleadings motion.[47] In making findings of fact and in applying the law to those facts the court is not obliged to accept as necessarily true allegations of fact that are rhetorical conclusions or that are inconsistent with the documents incorporated by reference.[48]

[127] The case law establishes that that issues that are novel, complex, and important should normally be decided on a full factual record after trial.[49] However, novelty by itself is not a reason to allow a cause of action to proceed to trial and a novel claim must also be arguable, have some elements of a cause of action recognized in law, be a reasonable and arguable incremental extension of established law and have a reasonable prospect of success.[50] In *Atlantic Lottery Corp. Inc. v. Babstock*,[51] the majority of the Supreme Court stated:

> [A] claim will not survive an application to strike simply because it is novel. It is beneficial, and indeed critical to the viability of civil justice and public access thereto that claims, including novel claims, which are doomed to fail be disposed of at an early stage in the proceedings. This is because such claims present "no legal justification for a protracted and expensive trial". If a court would not recognize a novel claim when the facts as pleaded are taken to be true, the claim is plainly doomed to fail and should be struck. [citation omitted]

[128] In the Ontario Court of Appeal's decision in *Darmar Farms Inc. v. Syngenta Canada Inc.*,[52] Justice Zarnett stated:

> 51. The fact that a claim is novel is not a sufficient reason to strike it. But the fact that a claim is novel is also not a sufficient reason to allow it to proceed; a novel claim must also be arguable. There must be a reasonable prospect that the claim will succeed.

[129] In developing the common law, courts are restrained to making incremental changes and leaving substantive change and radical development to the legislature or Parliament.[53] In *R. v.*

---

[46] *Ladas v. Apple Inc*., 2014 BCSC 1821 at para 59; *Arora v. Whirlpool Canada LP*, 2012 ONSC 4642 at para 12, aff'd aff'd 2013 ONCA 657, leave to appeal ref'd [2013] S.C.C.A. No. 498; *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42 at para. 22; *Stephen v. HMTQ*, 2008 BCSC 1656 at paras 48-49; *Folland v. Ontario* (2003), 64 OR (3d) 89 (C.A.); *Nash v. Ontario* (1995), 27 O.R. (3d) 1 (CA); *Canadian Pacific International Freight Services Ltd. v. Starber International Inc.* (1992), 44 C.P.R. (3d) 17 at para. 9 (Ont. Gen. Div.); *Canada v. Operation Dismantle Inc*., [1985] 1 S.C.R. 441; *A-G. Canada v. Inuit Tapirisat of Canada*, [1980] 2 S.C.R. 735.

[47] *Price v. Smith & Wesson Corp.*, 2021 ONSC 1114 at para 51; *Das v. George Weston Ltd.*, 2017 ONSC 4129 at paras. 14–29, aff'd 2018 ONCA 1053, leave to appeal refused [2019] S.C.C.A. No. 69; *Grenon v. Canada (Revenue Agency)*, 2016 ABQB 260 at para. 32; *.Deluca v. Canada (Attorney General)*, 2016 ONSC 3865; *Losier v. Mackay, Mackay & Peters Ltd.*, [2009] O.J. No. 3463 at paras. 39–40 (S.C.J.), aff'd 2010 ONCA 613, leave to appeal refused [2010] S.C.C.A. No. 438; *Merchant Law Group v. Canada (Revenue Agency)*, 2010 FCA 184 at para. 34.

[48] *Das v. George Weston Limited*, 2017 ONSC 4129 at paras. 27, 79-80, aff'd 2018 ONCA 1053.

[49] *Sells v. Manulife Securities Inc.*, 2014 ONSC 715; *Leek v. Vaidyanathan*, [2011] O.J. No. 200 at para. 3 (C.A.); *PDC 3 Limited Partnership v. Bregman + Hamann Architects*, [2001] O.J. No. 422 paras. 7–12 (C.A.).

[50] *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 19; *Darmar Farms Inc. v. Syngenta Canada Inc.*, 2019 ONCA 789 at para. 51; *Das v. George Weston Ltd.*, 2017 ONSC 4129 aff'd 2018 ONCA 1053, leave to appeal refused [2019] S.C.C.A. No. 69.

[51] 2020 SCC 19 at para. 19.

[52] 2019 ONCA 789 at para. 51.

[53] *Fraser River Pile & Dredge Ltd. v. Can-Dive Services Ltd.*, [1999] 3 S.C.R. 108 at para. 43; *London Drugs Ltd. v. Kuehne & Nagel International Ltd.*, [1992] 3 S.C.R. 299 at pp. 436–39, 461–62.*Watkins v. Olafson*, [1989] 2 S.C.R. 750.

Cuerrier,[54] Justice McLachlin, as she then was, stated: "This Court has established a rule for when it will effect changes to the common law. It will do so only where those changes are incremental developments of existing principle and where the consequences of the change are contained and predictable."

H. Intrusion upon Seclusion

[130] The Plaintiffs advance claims of intrusion upon seclusion against Ms. Thompson, Capital One, and Amazon Web.[55]

[131] In *Jones v. Tsige*,[56] in a judgment written by Justice Sharpe, the Ontario Court of Appeal (Winkler, CJO and Cunningham, ACJSC, *ad hoc*) ended the debate as to whether or not there were free-standing breach of privacy torts in Ontario.[57] Adopting the model described in American academic legal literature,[58] the Court of Appeal officially recognized four breach of privacy torts, one of which, misappropriation of personality, had already taken root in Ontario. The four breach of privacy torts were: (a) intrusion on seclusion, (b) public disclosure of embarrassing private facts, (c) publicity that places the plaintiff in a false light in the public eye, and (d) misappropriation of personality.

[132] The elements of intrusion on seclusion are: (1) the defendant without lawful justification intrudes physically or otherwise upon the seclusion of the plaintiff in his or her private affairs or concerns; (2) the defendant's intrusion is intentional or reckless; and (3) the invasion would be highly offensive causing distress, humiliation or anguish to a reasonable person.[59]

[133] The tort of intrusion on seclusion is only for significant invasions of personal privacy that, viewed objectively, a reasonable person would regard as highly offensive.[60] Proof of actual harm is not an element of the cause of action, and given the intangible nature of the interest protected, damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum.[61]

[134] In the immediate case, as against Ms. Thompson there is a legally viable cause of action for intrusion upon seclusion as against her. However, in the immediate case, it is plain and obvious that there is no viable claim for intrusion on seclusion as against Capital One or against Amazon Web.

[135] The intrusion on seclusion claims as against Capital One and Amazon Web are not legally viable for four reasons.

[136] First, it was Ms. Thompson who was the intruder. Capital One and Amazon Web are

---

[54] [1998] 2 S.C.R. 371 at para. 43.
[55] Fresh as Amended Statement of Claim, paragraphs 1©, 34, 54, 62, 82, 94, 114, 117, 118, 128, 131.
[56] 2012 ONCA 32.
[57] In *Somwar v. McDonald's Restaurants of Canada Ltd.* (2006), 79 O.R. (3d) 172 (S.C.J.) and *Nitsopoulos v. Wong* [2008] O.J. No. 3498 (S.C.J.), Justice Stinson and Justice Aston respectively held that it was not plain and obvious that there was no free-standing tort action for invasion of privacy.
[58] S.D. Warren & L.D. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. R. 193 and William L. Prosser, "Privacy" (1960), 48 Cal. L. R. 383.
[59] *Hopkins v. Kay*, 2014 ONSC 321, affd 2015 ONCA 112, leave to appeal to SCC refd. [2015] S.C.C.A. No. 157; *Jones v. Tsige*, 2012 ONCA 32.
[60] *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315 at paras. 137-139; *Jones v. Tsige*, 2012 ONCA 32 at para. 72.
[61] *Jones v. Tsige*, 2012 ONCA 32 at paras. 71-75.

alleged to have increased the risk of a data breach or to have failed to prevent the data breach. A failure to prevent an intrusion, even a reckless failure to prevent, is not an intrusion. Further, as I shall discuss below, Capital One and Amazon Web are not vicariously liable for Ms. Thompson's misconduct.

[137] During the course of the oral argument, the Plaintiffs' reliance on the certification motion decision in *Owsianik v. Equifax Canada Co.*,[62] dissipated. In the *Equifax* case, Justice Glustein had held that it was not plain and obvious that Equifax's alleged reckless and negligent failure to implement adequate cybersecurity could not satisfy the recklessness element of seclusion on intrusion and that it was not plain and obvious that a person who was reckless in facilitating an intrusion on seclusion could not also be liable for intrusion. A majority of the Divisional Court disagreed.[63] In the immediate case, I am bound to follow the decision of the Divisional Court. In the *Equifax* case, Justice Ramsey stated at para. 55:

> 55. I agree with my colleague (paragraph 43) that Equifax's actions, if proven, amount to conduct that a reasonable person could find to be highly offensive. But no one says that Equifax intruded, and that is the central element of the tort. The intrusion need not be intentional; it can be reckless. But it still has to be an intrusion. It is the intrusion that has to be intentional or reckless and the intrusion that has to be highly offensive. Otherwise, the tort assigns liability for a completely different category of conduct, a category that is adequately controlled by the tort of negligence.

[138] Adding to what Justice Ramsey said, I would add that if the tort of intrusion on seclusion would assign liability without an intrusion, then it would assign liability to categories of misconduct that are adequately controlled by an assortment of other possible torts, by statutory provisions, and by actions for breach of contract. The Court of Appeal in *Jones v. Tsige*, however, intended intrusion on seclusion to fill gaps in the law of privacy not pave them over.

[139] Second, assuming I am wrong and the alleged misdeeds of Capital One and of Amazon Web were an intrusion, then it was not an unauthorized intrusion. The Plaintiffs' pleadings that the applicants for credit did not authorize Capital One's retention of personal information on the servers of Amazon Web are not capable of proof because they are belied by the terms of the Application form and by the Credit Agreement and the Privacy Policy, which are incorporated by reference into the pleading. I have highlighted above the numerous provisions in the contract documents that address the uses that can be made with the personal information.

[140] Although the Plaintiffs plead that Capital One collected and used personal information for purposes to which the Class Members did not agree, the contract documents disprove this material fact. As a result, the causes of action, intrusion on seclusion, misappropriation of financial personality, breach of statutory causes of action, conversion, breach of confidence, breach of trust, breach of fiduciary duty, conversion, and strict liability that rely on that refuted material fact are certain to fail.

[141] Third, the alleged misconduct of Capital One and of Amazon Web alleged to constitute an intrusion on seclusion was not intentional or reckless, which are requisite constituent elements of the tort.

[142] The tort of intrusion on seclusion has a mental element of intentionality. The Plaintiffs' pleading seeks to elevate its copious allegations of negligence into recklessness, but carelessness

---

[62] 2019 ONSC 7110, *sub. nom Agnew-Americano v. Equifax Canada Co.*, leave to appeal to Div. Ct. granted, 2020 ONSC 5761 (Div. Ct.), var'd . 2021 ONSC 4112 (Div. Ct.).

[63] *Owsianik v. Equifax Canada Co.* 2021 ONSC 4112 (Div. Ct.)(McWatt ACJSCJ., Sachs and Ramsay JJ.), rev'g *sub. nom Agnew-Americano v. Equifax Canada Co.* on this point 2019 ONSC 7110

is not the same mental state as intentionality or recklessness. The Plaintiffs do not plead material facts that go beyond negligence, and as the discussion later in these Reasons for Decision reveals, there are proximity problems with the negligence claim against the Defendants, most particularly with respect to the negligence action against Amazon Web.

[143] As a legal concept, the notion of recklessness is well developed in the criminal and civil law jurisprudence, and it is a distinct and different kind of wrongdoing different from negligence. In *O'Grady v. Sparling*,[64] Justice Spence for the majority of Supreme Court of Canada stated: "The difference between recklessness and negligence is the difference between advertence and inadvertence; they are opposed, and it is a logical fallacy to suggest that recklessness is a degree of negligence."

[144] In *Jones v. Tsige*, in part to narrow the ambit of the tort, Justice Sharpe authenticated intrusion on seclusion as an intentional tort in which deliberate, wilful, purposeful, mindful, conduct by the defendant was a requisite constituent element and carelessness was insufficient to constitute the requisite intentionality.

[145] In *Broutzas v. Rouge Valley Health System*,[65] where a hospital was alleged to have been negligent in not preventing a nurse from accessing confidential medical records of childbearing patients to sell their contact information to marketers of registered education plans, I followed Justice Shape's lead when I declined to recognize negligence as a substitute for the recklessness that was the constituent element stipulated by the Court of Appeal. In *Broutzas*, I stated:

> 211. [A]s a matter of legal policy, courts should be hesitant to introduce or impose new liabilities particularly ones that would yield a flood of claims and undermine the law's careful regulation of liability. For example, in *Martel Building Ltd. v. Canada*, the Supreme Court declined to introduce a duty of care in contract bargaining, among other reasons, because to extend negligence law into the conduct of negotiations would encourage a multiplicity of needless lawsuits given the number of negotiations that do not culminate in a contract. Similarly, as a matter of legal policy, the introduction of a backstop negligence action for intrusion on seclusion against defendants at second and third degrees of proximity would undermine the careful work of the Court of Appeal in *Jones v. Tsige* to not open the floodgates of liability for intrusion on seclusion.

[146] The fourth flaw in the Plaintiffs' intrusion on seclusion claim is that while Ms. Thompson's conduct would be highly offensive causing distress, humiliation, or anguish to a reasonable person, the conduct of Capital One and Amazon Web was not highly offensive. As pleaded against them, Capital One's and Amazon Web's conduct amounts to making mistakes in safeguarding not particularly sensitive information that largely consists of information to identify the applicant for a credit card and to provide means to contact them. Capital One's or Amazon Web's conduct which might be wrongful and expose them to some other cause of action, is not offensive in the requisite legal sense that would constitute the tort of intrusion on seclusion.[66]

[147] I conclude that the Plaintiffs' cause of action for intrusion on seclusion does not satisfy the

---

[64] [1960] S.C.R. 804 at p. 808 (Kerwin C.J., Taschereau, Fauteux, Abbott, Martland, Judson and Ritchie JJ.: dissenting). See also: *Peracomo Inc. v. TELUS Communications Co*., 2014 SCC 29; *Hurst v. PricewaterhouseCoopers LLP*, [2009] O.J. No. 1415 (S.C.J.); *R. v. Gosset*, [1993] 3 S.C.R. 76; *R. v. Tutton*, [1989] 1 S.C.R. 1392; *Sansregret v. The Queen*, [1985] 1 S.C.R. 570.

[65] 2018 ONSC 6315 at para. 211.

[66] *Setoguchi v Uber B.V.* 2021 ABQB 18 at para. 52; *Wiseau Studio LLC v. Harper*, 2020 ONSC 2504; *Broutzas v. Rouge Valley Health System* 2018 ONSC 6315; *Larizza v. The Royal Bank of Canada*, 2017 ONSC 6140 at para. 59; aff'd 2018 ONCA 632; *Jones v. Tsige*, 2012 ONCA 32 at para. 72. See also: *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358 (2010); *Busse v. Motorola, Inc*. 351 Ill. App. 3d 67 (2004),

cause of action criterion as against Capital One and Amazon Web. These claims should be struck without leave to amend.

I. Misappropriation of Personality

[148] The Plaintiffs plead that Capital One and Amazon Web are liable for the privacy torts of (a) intentional misappropriation of financial personality; and (b) reckless misappropriation of financial personality.[67] In advancing these causes of action, the Plaintiffs would appear to be asking the court to extend the ambit of one of the four breach of privacy torts that was recognized by the Ontario Court of Appeal in *Jones v. Tsige*,[68] namely misappropriation of personality, which had already taken root in Ontario.[69]

[149] In advancing these causes of action, the Plaintiffs' thesis is that a Class Member's personality includes his or her unique financial personality which is a reflection of his or her character, traits, values, and behaviours. The Plaintiffs posit that without authorization, Capital One intentionally traded on the Class Members' financial personality by collecting and merchandizing the personal information for its own financial gain. The Plaintiffs submit that this trading on and exploitation of the financial personality of the class members caused and threatened to cause distress, humiliation, anguish, moral damages, and other damages to the Class Members and that Capital One perpetrated the tort of misappropriation of personality.

[150] With all due respect, the proposed cause of action for intentional or reckless misappropriation of personality is not remotely close to the existing tort of misappropriation of personality and cannot be an incremental extension of that tort.

[151] The gravamen of the existing tort is the usurpation of the plaintiff's right to control and market his or her personality.[70] More precisely, the gravamen of the tort is the usurpation of the plaintiff's right to be paid for testimonials and product endorsements. There has to be damage to a person's right to exploit his or her personality for commercial purposes. Thus, the tort has been typically employed by sports and entertainment celebrities, personalities who without the celebrity's permission have been represented as endorsing the defendant's goods or services.

[152] I will grant the Plaintiffs the notion that a person may have a unique financial personality. The celebrities who went from rags to riches or from riches to rags would be examples, but it is plain and obvious that the tort of misappropriation of personality is not available in the circumstances of the immediate case. In the immediate case there is nothing of an endorsement or testimonial in the Class Members' application for credit cards and filling out application forms. In the immediate case, there is no misappropriation and the Class Members consented to the gathering and the use of their financial information. In the immediate case, there is no use of the personal information to endorse Capital One's products or services. In the immediate case, there is no damage to the Class Members' right to exploit their personality for commercial purposes.

---

[67] Fresh as Amended Statement of Claim paragraphs 34, 54, 62, 82, 84, 94, 114, 128 and 131.
[68] 2012 ONCA 32.
[69] *Wiseau Studio, LLC v. Harper*, 2020 ONSC 2504; *Horton v. Tim Donut Ltd*., [1997] O.J. No. 4154 (C.A.); *Gould Estate v. Stoddard Publishing Co.*, (1996), 30 O.R. (3d) 520 (Gen. Div.), aff'd (1998), 39 O.R. (3d) 545 (C.A.), leave to appeal to S.C.C. ref'd [1998] S.C.C.A. No. 373; *Athans v. Canadian Adventure Camps Ltd*., [1977] O.J. No. 2417 (H.C.J.); *Krouse v. Chrysler Canada Ltd.* (1973), 1 O.R. (2d) 225 (C.A.), rev'g [1972] 2 O.R. 133 (H.C.J.). See also *Joseph v. Daniels* (1986), 4 B.C.LR. (2d) 239 (S.C.).
[70] *Hay v. Platinum Equities Inc*., 2012 ABQB 204 at para. 67.

[153] And, in the immediate case, in so far as Amazon Web is concerned, all it did is store bits and bytes of data on its servers, and it did not use or misuse any aspects of the Class Members' financial personality. It is pleaded that the Class Members did not even know that their personal information was being stored on Amazon Web's servers. Amazon Web certainly did not benefit from any testimonials that it should have to pay for.

[154] It is plain and obvious that in the immediate case, there are no causes of action for intentional misappropriation of financial personality or reckless misappropriation of financial personality. These claims should be struck without leave to amend.

J. Privacy Statutes

[155] The Plaintiffs plead a breach of data protection laws[71] and breach of s. 8 of the *Canadian Charter of Rights and Freedoms*[72] against Capital One and Amazon Web.

[156] Where a class action is brought in Ontario on behalf of a national class, it has become a convention to include statutes from other provinces and territories and from the federal government that may be available to the Class Members. In the immediate case, the Plaintiffs plead the privacy statutes from the provinces and territories and the *Charter*. Capital One and Amazon Web assert, however, that this court does not have jurisdiction with respect to three provinces (British Columbia, Manitoba, and Newfoundland and Labrador) because the statutes in those provinces expressly confer an exclusive jurisdiction on the domestic provincial court.

[157] There is merit to the Defendants' submission. As a constitutional law principle,[73] it is plain and obvious that this court has no jurisdiction with respect to the privacy statutes of British Columbia, Manitoba, and Newfoundland and Labrador.

[158] There are more problems with the Plaintiffs' statutory claims. A major problem for the Plaintiffs in advancing their statutory claims is that the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[74] the statute that the Plaintiffs would appear to rely on the most, does not grant a private right of action and is enforceable in the Federal Court not in a provincial court.

[159] PIPEDA sets out the circumstances in which an organization may collect, retain, and disclose personal information, and the purposes for which that information may be used. It establishes a Privacy Commissioner. The Act requires an organization to report to the Commissioner any breach of security safeguards involving personal information. The Commissioner, either acting upon a complaint or by initiating a complaint, has investigative powers. Upon the conclusion of an investigation, the Commissioner prepares a report including findings and recommendations. A person may complain to the Privacy Commissioner who may conduct an investigation of the complaint. The Privacy Commissioner may issue a report making recommendations on how to resolve the complaint. The Privacy Commissioner, however, is not empowered to award damages. Only if a person makes a complaint to the Privacy Commissioner,

---

[71] Fresh as Amended Statement of Claim paragraphs 28, 35, 36, 38, 39, 41, 46, 50, 51, 53, 54, 55, 58, 62, 76, 77, 85, 86, 92, 98, 114, 116.
[72] Fresh as Amended Statement of Claim 34, 36, 58, 62, 85, 130.
[73] *Butt v. Kiewit Energy Corporation*, 2019 NLSC 119 at para. 76; *Douez v. Facebook, Inc.*, 2014 BCSC 953 at para. 78, aff'd on other grounds 2017 SCC 33; *Gould v. Western Coal Corporation*, 2012 ONSC 5184 at paras. 319-339; *Petrov v. B.C. Ferry Corp*., 2003 BCSC 270 at para. 47.
[74] 2000, c. 5.

then the complainant may also have a hearing in the Federal Court and the Federal Court, among other remedies, may award damages including damages for humiliation.[75]

[160] It is for the Federal Court not this court to award damages for violations of PIPEDA.

[161] There are still more problems with the Plaintiffs' statutory claims; visualize:

a. The Federal *Privacy Act*,[76] applies only when personal information is collected by a government institution. However, Capital One and Amazon Web operate in the private sector, and they are not government institutions.

b. Alberta's *Freedom of Information and Protection of Privacy Act*;[77] New Brunswick's *Right of Information and Protection of Privacy Act*;[78] North West Territories' *Access to Information and Privacy Act*;[79] Nova Scotia's *Freedom of Information and Protection of Privacy Act*;[80] Nunavut's *Access to Information and Privacy Act*;[81] Ontario's *Freedom of Information and Protection of Privacy Act*;[82] Prince Edward Island's *Freedom of Information and Protection of Privacy Act*;[83] Québec's *Act Respecting the Protection of Personal Information in the Private Sector*;[84] and Yukon's *Access to Information and Protection of Privacy Act*,[85] govern the public's right to access government information, and although these statutes are pleaded, the immediate case has nothing to do with access to information from the government.

c. While the Plaintiffs' references to the *Canadian Charter of Rights and Freedoms* is perhaps useful insofar as it demonstrates that the right to privacy has developed a quasi-constitutional importance, the *Charter* does not apply to actors in the private sector, unless the actor is performing some specific government function or acting as a government agent, and it is not sufficient that the actor is carrying out some purpose that is regulated and for the public good.[86] In the immediate case, Capital One and Amazon Web are not government actors.

[162] Dealing directly with any possibly applicable statutory provisions, it first needs to be noted that as is well established, there is no nominate tort of statutory breach. In the absence of relevant statutory causes of action, any privacy legislation could only serve as basis for establishing a standard of care in negligence.[87]

[163] As for the possibly relevant statutory provisions, in the immediate case there is merit in Capital One's and Amazon Web's submission that it is plain and obvious that the Plaintiffs' claim

---

[75] *Englander v. Telus Communications Inc*, 2004 FCA 387.
[76] R.S.C. 1985, c. P-21.
[77] R.S.A. 2000, c. F-25.
[78] S.N.B. 2009, c. R-10.6.
[79] S.N.W.T. 1994, c. 20.
[80] S.N.S. 1993, c. 5.
[81] S.N.W.T. (Nu) 1994, c. 20.
[82] R.S.O. 1990, c. F.31.
[83] R.S.P.E.I. 1998, c. F-15.01.
[84] R.S.Q., c. P-39.1.
[85] R.S.Y. 2002, c. 1.
[86] *McKitty (Litigation guardian of) v. Hayani*, 2019 ONCA 805 at para. 49; *R. v. Buhay*, 2003 SCC 30 at para. 25; *Eldridge v. British Columbia (Attorney General)*, [1997] 3 S.C.R. 624 at para. 43; *McKinney v. University of Guelph*, [1990] 3 S.C.R. 229 at p. 269.
[87] *R. v. Saskatchewan Wheat Pool*, [1983] 1 S.C.R. 205.

of a breach of any of privacy statutes would fail because it is a constituent element of all these statutes that the defendant's conduct was wilful; however, the pleaded material facts of the Fresh as Amended Statement of Claim do not amount to wilfulness such as to violate the Class Members' rights of privacy. It is not willfulness to fail to prevent a third party from invading another's privacy.

[164] In other words, as discussed above in the context of the tort of intrusion on seclusion, the alleged misconduct of Capital One and Amazon Web wants for the intentionality that would satisfy the constituent elements of the statutory privacy torts. The case law under the provincial privacy statutes establishes that where an element of the statutory privacy tort is that the defendant's violation was wilful, the plaintiff must show that the defendant's conduct was a purposeful violation of the plaintiff's privacy; wilful means more than the defendant did an act that violated the plaintiff's privacy or that the defendant carelessly or accidentally caused the plaintiff's privacy to be breached, and the plaintiff must show that the defendant knew that his or her conduct would violate the plaintiff's privacy.[88] The facts pleaded in the Fresh as Amended Statement of Claim contradict any notion that the defendants intended to invade the Class Members' privacy and breached the statutory privacy torts.

[165] I conclude that it is plain and obvious that the Plaintiffs have not pleaded and could not plead the material facts for a statutory cause of action for breach of privacy.

[166] In any event, in oral argument, Class Counsel explained that the numerous statutes including the privacy acts of various provinces that had been pleaded were relevant to the theory of the case not so much because they were severally actionable but for a different reason. The Plaintiffs submitted that the relevance of these statutes was that the Defendants had admitted that they were bound by Canadian law, and thus, the Defendants' breaches of the provincial statutes and of PIPEDA established the intentional conduct that were prerequisites to intrusion on seclusion, conversion, and strict liability, and these breaches were also contract breaches for those Class Members who had contracts.

[167] This argument from the Plaintiffs more hinders that it assists the Plaintiffs. The argument confirms that they are not serious about certifying the statutory claims as free-standing causes of action that would satisfy section 5(1)(a) of the *Class Proceedings Act*, and it reveals that the Plaintiffs have not pleaded the material facts necessary to establish the mental elements of intrusion on seclusion, misappropriation of personality, conversion, or the privacy statutes. The Plaintiffs' argument reveals a failed attempt to bootstrap their common law causes of action with statutory causes of action that are not jurisdictionally or factually available or applicable.

[168] For the above reasons, I conclude that it is plain and obvious that the Plaintiffs do not have a viable cause of action for the violation of the privacy statutes of other provinces or of the federal government. These claims should be struck out without leave to amend.

---

[88] *Kumar v. Korpan*, 2020 SKQB 256 at paras. 30-36; *Duncan v. Lessing*, 2018 BCCA 9; *Cole v Prairie Centre Credit Union Ltd.*, 2007 SKQB 330; *Watts v. Klaemt*, 2007 BCSC 662; *Hollinsworth v BCTV*, [1999] 6 WWR 54 (B.C.C.A.); *Peters-Brown v Regina District Health Board*, [1996] 1 WWR 337 (Sask. Q.B.) aff'd [1997] 1 WWR 638 (Sask. C.A.).

K. Conversion

[169] The Plaintiffs plead that Capital One and Amazon Web committed the tort of conversion.[89]

[170] The elements of a claim for conversion are: (1) the plaintiff has an immediate right to possession of personal property; (2) the personal property is identifiable or specific; and (3) the defendant takes, uses, or destroys the goods or interferes with the plaintiff's right of possession.[90]

[171] It is plain and obvious the claim for conversion is untenable and bound to fail. There are five reasons.

[172] First, the tort of conversion does not apply to information, intellectual or intangible property. Such property does not entail a right of possession.

[173] There are torts or legal remedies that do apply to provide remedies for the misappropriation and misuse of intellectual property that do not involve the notion of possession or tangible property; for example, there is breach of confidence (discussed later in these Reasons for Decision). However, advancing a claim for conversion is a *non sequitur* in the circumstances of the immediate case. Information is not a type of property within the ambit of the tort of conversion which is for tangible, not intangible, property.[91] The misuse of private information might be amenable to a breach of confidence, but that is a misuse of information not a conversion of it.

[174] The Plaintiffs relied on the British Columbia decision *Canivate Growing Systems Ltd. v. Brazier*,[92] where Justice Baker found the Defendants liable for breach of fiduciary duty, passing off, and conversion, but not breach of trademark, and where she stated at paragraph 71:

> 71. In the electronic age in which we live, I find that it would be incongruous if conversion were limited to physical goods, or tangible chattels. In the case at bar, the defendant exerted exclusive control over Canivate's website as soon as he removed administrative control of canivate.com from the company. The defendant held the only key to the website which was critical to operations of the company and prevented Canivate from using its website and email addresses. I find that a modern conception of conversion must include wrongful interference with intangible goods, such as electronic data, websites and email.

[175] Justice Baker's decision dealt with a case in which the plaintiff had personal information that he owned and controlled – his business's web page domain name, the business's web page, and the email account for his commercial business. The element of control was something akin to possession of those business assets. There is nothing remotely like that element of control over a person's name which is normally put out in the world to be used. Thus, apart from the fact that I am not bound by *Canivate Growing Systems Ltd.*, it is distinguishable from the immediate case and does not detract from the law that does bind me that conversion does not sound in the circumstances of the immediate case.

---

[89] Fresh as Amended Statement of Claim paragraphs 11, 34, 41, 54, 58, 84, 94, 106, 117 and 128.
[90] *UBS Wireless Services Inc. v. Inukshuk Wireless Partnership*, [2008] O.J. No. 1704 (S.C.J.); *DaimlerChrysler Canada Inc. v. Associated Bailiffs &Co.*, [2005] O.J. No. 2855 (S.C.J.); *373409 Alberta Ltd. (Receiver of) v. Bank of Montreal*, 2002 SCC 81; *Kingston Technology Co. v. Orr*, [2000] O.J. No. 3959 (S.C.J.); *Boma Manufacturing Ltd. v. Canadian Imperial Bank of Commerce*, [1996] 3 S.C.R. 727; *McLean v. Bradley* (1878), 2 S.C.R. 535.
[91] *ResourceEye Services Inc. v. Atrum Coal Groundhog Inc.* 2015 BCSC 821 at paras. 44-50; *MacDonnell v. Halifax Herald Ltd.*, 2009 NSSC 187; *K.R. Thompson Engineering Ltd. v. Webster* (1980), 31 N.B.R. (2d) 329 at paras. 30-34 (Q.B.)
[92] 2020 BCSC 232

[176] The Ontario case of *Prim8 Group Inc. v. Tisi*,[93] also relied on by the Plaintiffs, is similarly not helpful to them. In that case, a former director and officer removed the computer with the proprietary software that the plaintiffs used in their business. Justice Lococo quickly dealt with the claim for conversion by saying that a person is liable for the tort of conversion if that person wrongfully interferes with the goods of another in a manner that is inconsistent with the rights of the true owner. I have no reason to doubt the correctness of Justice Lococo's decision, but unlike the immediate case, in *Prim8 Group Inc. v. Tisi*, there was an interference over goods that the plaintiffs controlled in a manner that was inconsistent with the true owner's rights. The case is not authority that the tort of conversion is generally available for personal contact and identification information that is data on a computer server.

[177] Second, in any event, the Class Members' rights to their own personal information was not interfered with in the immediate case. In the immediate case, the Class Members still have access to their personal information and so their right to possess it is not interfered with. The Class Members obviously retained the use of their personal information.

[178] Third, for there to be a conversion of the personal property, the property must be damaged in some way,[94] which is not the situation in the immediate case. The personal information of a person's name or contact information was not damaged in the immediate case.

[179] Fourth, Capital One's and Amazon Web's use of the Class Members' personal information was not wrongful. Their use of the information was consensual and based on the Application for Credit and the Cardholder Agreements, both of which incorporate Capital One's Privacy Policy authorizing the use of the personal information for many purposes.

[180] Fifth, conversion is an intentional tort and involves a deliberate interference with the right of possession.[95] For all the reasons set out above in the discussion about intrusion on seclusion and the statutory causes of action, there was no intentional or deliberate acts with respect to the Class Members' personal information. The alleged negligent storing of the Class Members' data does not satisfy the test for conversion.

[181] For the above reasons, I conclude that it is plain and obvious that the Plaintiffs do not have a viable cause of action for conversion. This claim should be struck out without leave to amend.

L. Breach of Confidence, Trust and Fiduciary Duty

[182] The Plaintiffs plead against Capital One the causes of action of breach of confidence, trust, and fiduciary duty.[96]

[183] The elements of a breach of confidence are: (1) the plaintiff imparts information having a quality of confidence (confidential information); (2) the information was imparted in circumstances in which an obligation of confidentiality arises (communication in confidence); and

---

[93] 2016 ONSC 5662

[94] *Genesis Fertility Centre Inc. v. Yuzpe*, 2019 BCSC 233 at para. 234; *BMW Canada Inc. (Alphera Financial Services Canada) v. Mirzai*, 2018 ONSC 180 at para. 26.

[95] *AVS Transport Inc. v. van Ravenswaay*, 2016 ONSC 3568; *Northstar Leasing Corp. v. Two Ten Spruce Corp.*, [2007] O.J. No. 1068 (S.C.J.); *CIT Financial Ltd. v. 1153461 Ontario Inc.*, [2004] O.J. No 3308 (S.C.J.).

[96] Fresh as Amended Statement of Claim paragraphs 1(c), 10, 11, 21, 29, 30, 34, 41, 46, 50, 51, 53, 54, 58, 62, 76, 82, 84, 86, 94, 106, 114, 117, 128, 129.

(3) the defendant makes an unauthorized use of the information (misuse of information).[97]

[184] The elements of a claim for breach of fiduciary duty are: (1) a fiduciary relationship: (2) a fiduciary duty; and (3) breach of the fiduciary duty.[98]

[185] The Plaintiffs' theory for their breach of confidence, trust, and fiduciary duty claims is that Capital One gained unilateral control over the Class Members' confidential personal information and the Class Members became vulnerable and "were at the mercy of Capital One" which assumed the role of a fiduciary with respect to the treatment of the personal information. The Plaintiffs posit that Capital One's fiduciary duties required Capital One to either return the data after its single purpose use or to comply with the data protection laws of Canada, including duties not to misuse the data as its own asset. The Plaintiffs submit that Capital One did not return the data and therefore breached confidence and its fiduciary duties by: (a) using the data internally and externally to acquire revenue for Capital One's business enterprise; (b) negligently storing the data; and (c) unlawfully migrating and aggregating the Class Members' data in the United States on Amazon Web's computers where the data became a target for criminals, which inevitably lead to the data breach that took place in April 2019.

[186] It is, however, plain and obvious that the Plaintiffs have not pleaded and cannot plead legally viable causes of action for breach of confidence, trust, and fiduciary duty. The Plaintiffs' theory is fallacious.

[187] Fiduciary duties arise in one of two ways. First, some relationships are categorically fiduciary relationships with attendant fiduciary duties. Historically, the law has recognized certain relationships as categorically fiduciary in nature; trustee-beneficiary, lawyer-client, principle-agent, parent-child, guardian-ward are the main examples. Second, some relationships are situationally fiduciary, which is to say that when certain circumstances exist, the law recognizes an *ad hoc* fiduciary relationship with attendant duties. *Ad hoc* fiduciary relationships must be established on a case-by-case basis.[99]

[188] The indicia for an *ad hoc* fiduciary relationship, which are not a comprehensive code, but rather guidance to a court in analyzing the legal classification of a relationship are: (a) the alleged fiduciary has scope for the exercise of some discretion or power; (b) the alleged fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal interest; (c) the alleged beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power; and (d) the alleged fiduciary either implicitly or expressly has undertaken or accepted a responsibility to act in the best interest of the alleged beneficiary and to act in accordance with a duty of loyalty. The degree of discretionary control must be equivalent or analogous to direct administration of that interest.[100]

[189] In *Alberta v. Elder Advocates of Alberta Society*,[101] Chief Justice McLachlin stated:

---

[97] *Cadbury Schweppes Inc. v. FBI Foods Ltd*., [1999], 1 S.C.R. 142*; Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574; *Coco v. A. N. Clark (Engineers) Ltd*., [1969] R.P.C. 41 (Ch.).
[98] *Galambos v. Perez*, 2009 SCC 48 at para. 37; *Hodgkinson v. Simms*, [1994] 3 S.C.R. 377; *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574; *Frame v. Smith*, [1987] 2 S.C.R. 99; *Canadian Aero Services Ltd. v. O'Malley*, [1974] S.C.R. 592 at p. 616.
[99] *Alberta v. Elder Advocates of Alberta Society*, 2011 SCC 24 at para. 33.
[100] *Brown v. Canada (Attorney General)*, 2017 ONSC 251 at para. 67; *Alberta v. Elder Advocates of Alberta Society*, 2011 SCC 24 at para. 53.
[101] 2011 SCC 24 at para. 36.

> 36. In summary, for an *ad hoc* fiduciary duty to arise, the claimant must show, in addition to the vulnerability arising from the relationship as described by Wilson J. in *Frame:* (l) an undertaking by the alleged fiduciary to act in the best interests of the alleged beneficiary or beneficiaries; (2) a defined person or class of persons vulnerable to a fiduciary's control (the beneficiary or beneficiaries); and (3) a legal or substantial practical interest of the beneficiary or beneficiaries that stands to be adversely affected by the alleged fiduciary's exercise of discretion or control.

[190] The critical constituent element of a fiduciary relationship is that the fiduciary forsakes or subrogates his or her personal interests in favour of the beneficiary of the relationship.[102]

[191] In the immediate case, it appears that the Plaintiffs accept, as recognized by the jurisprudence, that the relationship between a bank and its customers is a contractual or a debtor and creditor relationship and not a fiduciary relationship.[103] The Plaintiffs, rather, rely on an *ad hoc* fiduciary relationship arising with every Class Member. However, the material facts pleaded of the Class Members that could be pleaded in individual cases and or on a class-wide basis do not establish that Capital One relinquished its own self-interest and agreed to act on behalf of those persons applying for its credit cards. There is no fiduciary relationship.

[192] While Capital One undertook obligations with respect to the confidential information of the applicants, that undertaking was not for a single use purpose as is demonstrated by the credit card application and by the credit card agreement that are incorporated by reference into the pleaded material facts. Capital One's obligations were contractual not fiduciary.

[193] The Class Members were adults applying for credit cards, and while it may be some of them were of modest means, it is certainly not the case that six million Canadians were vulnerable in the requisite sense for a fiduciary relationship. Whatever contractual undertaking Capital One made, it did not make the Class Members vulnerable as the Plaintiffs in their mistaken version of how a fiduciary relationship is established would have it.

[194] Further even assuming that an *ad hoc* fiduciary relationship was established in the immediate case for six million Canadians, there was no breach of fiduciary duty because the six million Canadians signed contracts authorizing Capital One to make use of the personal information for more than a single spent purpose of applying for a credit card.

[195] As for the Plaintiffs' pleading of breach of trust, it makes no sense. There is no trust - express, implied, constructive - resulting in the immediate case, and there is no trust corpus.

[196] Further, even if in the immediate case there was a trust with respect to the Class Members' personal information, then the material facts incorporated by reference into the Fresh as Amended Statement of Claim reveal that there was no breach of trust because the Class Members authorized uses for the personal information beyond the alleged single purpose use of applying for a credit card.

[197] Pleading a breach of confidence makes some sense in the immediate case, but there is no basis for it based on the material facts pleaded or that could be pleaded against Capital One or Amazon Web because most of the information was not confidential and Capital One and Amazon

---

[102] *Catalyst Capital Group Inc. v. Dundee Kilmer Developments Limited*, 2016 ONSC 6778; *Professional Institute of the Public Service of Canada (Attorney General)*, 2012 SCC 71; *Alberta v. Elder Advocates of Alberta Society*, 2011 SCC 24

[103] *Evans v. Bank of Nova Scotia*, 2014 ONSC 2135 at paras. 39-44; *Balswin v. Daubney* (2006), 83 OR. (3d) 308 (C.A.); *Pierce v. Canada Trustco Mortgage Co*., [2005] O.J. No. 1886 (C.A.)

Web did not make an unauthorized use of the information. There was no misuse of information.[104]

[198] For these Reasons, I strike the claims for breach of confidence, trust, and fiduciary duty without leave to amend.

M. Strict Liability

[199] The Plaintiffs plead strict liability as against Capital One and Amazon Web.[105] Relying on academic literature,[106] the Plaintiffs assert that their data breach cause of action is and ought to be treated as a modern extension of strict liability as formulated by the land law cause of action known as *Rylands v. Fletcher*,[107] which is traditionally associated with the land law torts of trespass, negligence, and nuisance but not to personal property where negligence principles of product liability govern without the imposition of strict liability.[108]

[200] The cause of action known as *Rylands v. Fletcher* postulates that a person who makes a non-natural use of his or her land brings on to his or her property something that will cause harm if it escapes from the property is liable for the damage caused if the thing escapes.[109]

[201] The Plaintiffs' argument is that just as the strict liability rule of *Rylands v. Fletcher* was a development of the industrial revolution where the law was called on to regulate the industrial uses that were important for economic development but that could also cause harm, the law must now regulate the use of data because data is the energy of the machine learning and artificial intelligence technologies of the information technology revolution that is transforming society.

[202] Before getting to the legal merits of this argument, as a policy argument it fails abysmally, because it incorrectly assumes or posits that the law does not already adequately regulate the collection and use of data,[110] and the policy argument also fails to provide any justification to explain why strict liability would be required as the regulatory tool.

[203] As it is, the Plaintiffs plead myriad statutory and common law privacy regulations that do not support their submission that a new strict liability regime is called for. Moreover, in addition to the myriad causes of actions that in appropriate circumstances could be used to protect privacy and information, there are also copyright, trademark, and patent protections and the torts of defamation, passing off, slander of title, fraud, and misrepresentation. There is no regulatory gap to fill.

[204] Moreover, as I shall explain later in these Reasons for Decision, the Plaintiffs forswear the

---

[104] *Cadbury Schweppes Inc. v. FBI Foods Ltd*., [1999], 1 S.C.R. 142*; Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574; *Coco v. A. N. Clark (Engineers) Ltd*., [1969] R.P.C. 41 (Ch.).
[105] Fresh as Amended Statement of Claim paragraphs 123 and 131.
[106] *Rylands v. Fletcher* (1866), L.R. 1 Ex. 265, aff'd (1868), L.R. 3 H.L. 330.
[107] Danielle Keats Citron, "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age", (2007) 80 S.Cal.L.Rev 241. Agrawal, Ajay, Joshua Gans & Avi Goldfarb, Prediction machines: the simple economics of artificial intelligence, (Boston, MA: Harvard Business Review Press, 2018).
[108] *Price v. Smith & Wesson Corp*., 2021 ONSC 1114 at para 111; *St Isidore Co-Op Limited v AG Growth International Inc*, 2019 ABQB 763 at para. 38, aff'd 2020 ABCA 447 at para. 22; *McCluskey v. Ford Motor Co*., 2017 PESC 17 at para. 26; *Baker v. Suzuki Motors Co*. (1993), 12 Alta LR (3d) 193 (Q.B.) at para. 77; *Dahlberg v. Naydiuk*, (1969), 72 W.W.R.(N.S.) 210 (Man. C.A.); *Ayoub v. Beaupre* [1964] S.C.R. 448; *Read v. J. Lyons & Co*., [1947] A.C. 156.
[109] *Smith v. Inco Limited*, 2011 ONCA 628; *Gersten v. Municipality of Metropolitan Toronto* (1973), 2 O.R. (2d) 1 (H.C.J.); *Rylands v. Fletcher* (1866), L.R. 1 Ex. 265, aff'd (1868), L.R. 3 H.L. 330.
[110] There is also criminal law. See for instance Part VI (Invasion of Privacy) of the *Criminal Code*, R.S.C. 1985, c. C-46.

straightforward breach of contract claims that might have been available to them. From a policy perspective that cause of action would appear to be adequate for the immediate case, without inventing a new form of strict liability. And in this regard, it may be observed that breach of contract is already a strict liability regime that does not have proof of damages or any mental state as constituent elements.

[205] Turning then to the legal merits of this argument, it is plain and obvious that this extension or adaption of land law to intellectual property law is foreclosed. In *Smith v. Inco Limited*,[111] the Court of Appeal held that, despite having support among academic writers, there was no basis for this extension of strict liability law.

[206] Moreover, even if the doctrine were extended in the immediate case, it would not be available to the majority of the Class Members who have suffered no damages from the data breach and damage is a prerequisite of a claim relying on *Rylands v. Fletcher*.

[207] For these Reasons, I strike the strict liability claims without leave to amend.

N. Vicarious Liability

[208] The Plaintiffs plead that Capital One and Amazon Web are vicariously liable for Ms. Thompson's breach of confidence, breach of trust, breach of privacy, intentional and/or reckless intrusion upon seclusion, misappropriation of the identity and conversion of the confidential data.

[209] It is plain and obvious that Capital One and Amazon Web are not vicariously liable for Ms. Thompson's wrongdoings however those wrongdoings are classified.

[210] The constituent elements of a claim of vicarious liability are: (1) that there must be a close enough relationship between the employer and the tortfeasor that it would be appropriate to impose vicarious liability; and (2) the tortfeasor's wrong is so connected with his or her employment that it can be said that the employer has introduced the risk of the wrong.[112]

[211] In *Bazley v. Curry*,[113] the Supreme Court of Canada held that the fundamental question of vicarious liability is whether the wrongful intentional act by an employee was sufficiently related to conduct authorized by the employer to justify the imposition of liability. In considering whether there is a sufficient connection between the wrongful conduct and the conduct authorized by the employer, the following five factors are relevant: (a) the opportunity that the enterprise afforded the employee to abuse his or her power; (b) the extent to which the wrongful act may have furthered the employer's aims (and hence be more likely to have been committed by the employee); (c) the extent to which the wrong was related to friction, confrontation or intimacy inherent in the employer's enterprise; (d) the extent of power conferred on the employee in relation to the victim; and (e) the vulnerability of potential victims to wrongful exercise of the employee's power.

[212] In *Bazley v. Curry*, the Court stated that there must be a strong connection between what the employer was asking the employee to do and the wrongful act. It must be possible to say that the employer significantly increased the risk of the harm by putting the employee in his or her position and requiring the employee to perform the assigned tasks. In the companion case of *KLB*

---

[111] 2011 ONCA 62.

[112] *M.B. v. British Columbia*, 2003 SCC 53*E.D.G. v. Hammer*, 2003 SCC 52; *K.L.B. v. British Columbia*, 2003 SCC 51; *671122 Ontario Ltd. v. Sagaz Industries Canada Inc*., [2001] 2 S.C.R. 983; *Jacobi v. Griffiths*, [1999] 2 S.C.R. 570; *Bazley v. Curry*, [1999] 2 S.C.R. 534; *London Drugs Ltd. v. Kuehne & Nagel International Ltd*., [1992] 3 S.C.R. 299.

[113] [1999] 2 SCR 534. See also *KLB v. British Columbia*, 2003 SCC 51.

v British Columbia,[114] the Court stated that a mere opportunity to commit a tort created by virtue of employment does not suffice to impose vicarious liability.

[213] In the immediate case from a factual perspective, it should be noted that Ms. Thompson is not alleged to have done anything wrong during her employment by Amazon Web and she clearly was not an employee of Capital One when she hacked the data base.

[214] With this recitation of the law associated with vicarious liability in mind and with an understanding of the facts, it becomes apparent from the pleaded material facts of the Fresh as Amended Statement of Claim that in the immediate case, the Plaintiffs are seeking to apply a law designed to impose liability on an employer for the acts of its employee in the course of employment as a means to impose liability on an employer (Amazon Web) and on a customer of the employer (Capital One) for the acts of a former employee (Ms. Thompson) in the course of her after-employment. There is no precedent for such a cause of action, and it is no incremental extension of the common law and would be a paradigm shift.

[215] Although there are authorities,[115] it would seem trite to say without the need to cite authorities that a person should not be liable for another's wrongdoing unless they are somehow implicated in that wrongdoing, but the Plaintiffs' purported claim of vicarious liability ignores this triteness because the Defendants were no longer connected to Ms. Thompson who was no longer employed by Amazon Web.

[216] It would seem trite to say without the need to cite authorities that an employer has never been held liable for the activities of an employee outside of his or her employment,[116] much less for the activities of a former employee post-employment, but the Plaintiffs' claim in vicarious liability ignores this triteness. The lynchpin of vicarious liability is that the employee's wrongdoing was in the course of employment. More than just having or having had an employment relationship is needed to establish vicarious liability.

[217] It would seem trite to say without the need to cite authorities that the law would be both absurd and unfair if it imposed liability on a defendant for failing to do the impossible. In the immediate case, it is plain and obvious that it would be both absurd and unfair to impose liability (a) on Amazon Web for its failure supervise a former employee for her post-employment activity; or, (b) on Capital One for its failure to supervise someone else's former employee from wrongdoing in her post-employment activity.

[218] For all these reasons, the claim for vicarious liability should be struck without leave to amend.

O. Negligence and Duty to Warn

[219] The Plaintiffs plead that Capital One and Amazon Web are liable for negligence[117] and for a breach of the duty to warn.[118] In the context of the Plaintiffs' misappropriation and misuse of

---

[114] 2003 SCC 51.
[115] *Martin v. Astrazeneca Pharmaceuticals Plc*, 2012 ONSC 2744, aff'd 2013 ONSC 1169 (Div. Ct.); *Fullowka v Royal Oak Ventures Inc*., 2008 NWTCA 4, aff'd 2010 SCC 5.
[116] *Aviva Canada Inc. v. Lyons Auto Body Limited*, 2019 ONSC 6778; *Bazley v. Curry*, [1999] 2 S.C.R. 534.
[117] Fresh as Amended Statement of Claim paragraphs 1(c), 1(e), 11, 21, 84, 85, 106, 114, 116, 117, 118, 119, 128.
[118] Fresh as Amended Statement of Claim paragraphs 1(c), 11, 18, 31, 38(viii), 38(x), 41, 54, 58, 76, 81, 82, 84, 98, 101, 102, 103, 104, 106, 107, 109, 111, 113, 114, 116, 117, 128.

data case, the duty to warn claim sounds as a novel negligence cause of action.

[220] With respect to the duty to warn, the Plaintiffs allege in the Fresh as Amended Statement of Claim that Capital One had the duty to warn the Class Members: (a) of the increasing risk of the inevitable data breach; (b) of the increased risk if their data was retained and stored rather than returned after the singular use of applying for a credit card; (c) of the increased risk of a data breach because the data had been migrated to the U.S.; (d) of the increased risk due to continuing technical changes at Capital One and Amazon Web; (e) of the event of Ms. Thompson's cyber security attack when it occurred; (f) of the event of Ms. Thompson's posting of the data on GitHub when it occurred; and (g) of the event of the publication of the Class Members' data on the World Wide Web.

[221] In a guilt by association, the Plaintiffs plead in their Fresh as Amended Statement of Claim that "Amazon Web, by accepting that Capital One owned the confidential data as its own asset, legally adopted all of the Capital One duties of care, duties to warn […]".

[222] As I shall now explain, it is plain and obvious that the Plaintiffs and the Class Members do not have legally viable and certifiable causes of action for negligence or for a breach of a duty to warn. The analysis may begin by noting that the constituent elements of a claim in negligence are: (1) the defendant owes the plaintiff a duty of care; (2) the defendant's behaviour breached the standard of care; (3) the plaintiff suffered compensable damages; (4) the damages were caused in fact by the defendant's breach; and, (5) the damages are not too remote in law.[119]

[223] In the immediate case, the third constituent element of negligence (compensable harm) is significant to the analysis of whether the Plaintiffs have pleaded a legally viable cause of action. The compensable harm constituent element is particularly important because the overwhelming majority of the six million Canadians affected by the data breach will not have suffered harm compensable by the tort of negligence.

[224] The overwhelming majority of the six million Canadians affected by the data breach will not have suffered any compensable damages because negligence law does not recognize as compensable harm upset, disgust, anxiety, agitation or mere psychological upset that does not cause a serious and prolonged injury and that does do not rise above the ordinary annoyances, anxieties and fears that people living in society routinely experience.[120] (This was the gap in the law filled by *Jones v. Tsige*,[121] allowing compensation if the invasion would be highly offensive causing distress, humiliation or anguish to a reasonable person.)

[225] The overwhelming majority of the six million Canadians affected by the data breach will not have suffered any compensable damages because negligence law does not recognize as compensable harm the risk of injury or harm or the increased risk of harm or injury.[122]

[226] In the immediate case, the overwhelming majority of the six million Canadians will suffer no injury at all and for the minority who do suffer harm their losses will be pure economic losses.

---

[119] *Saadati v. Moorhead*, 2017 SCC 28; *Mustapha v. Culligan of Canada Ltd*., 2008 SCC 27.
[120] *Setoguchi v Uber B.V.* 2021 ABQB 18; *Stewart v. Demme*, 2020 ONSC 83; *Li v. Equifax* 2019 QCCS 4340; *Bourbonnière c. Yahoo! Inc.* 2019 QCCS 2624; *Condon v. Canada*, 2014 FC 250, var'd on other grounds 2015 FCA 159; *Mazzonna c. DaimlerChrysler Financial Services Canada Inc.* 2012 QCCS 958*; Saadati v. Moorhead*, 2017 SCC 28; *Mustapha v. Culligan of Canada Ltd*., 2008 SCC 27.
[121] 2012 ONCA 32.
[122] *Setoguchi v Uber B.V* 2021 ABQB 18; *Atlantic Lottery Corp. Inc. v. Babstock*, 2020 SCC 19 at para. 33.

However, tort claims for pure economic losses are only available in rare circumstances.[123]

[227] In *Martel Building Ltd. v. Canada,*[124] Justices Iacobucci and Major stated for the Supreme Court of Canada at para. 37:

> Over time, the traditional rule was reconsidered. In *Rivtow* and subsequent cases it has been recognized that in limited circumstances damages for economic loss absent physical or proprietary harm may be recovered. The circumstances in which such damages have been awarded to date are few. To a large extent, this caution derives from the same policy rationale that supported the traditional approach not to recognize the claim at all. First, economic interests are viewed as less compelling of protection than bodily security or proprietary interests. Second, an unbridled recognition of economic loss raises the spectre of indeterminate liability. Third, economic losses often arise in a commercial context, where they are often an inherent business risk best guarded against by the party on whom they fall through such means as insurance. Finally, allowing the recovery of economic loss through tort has been seen to encourage a multiplicity of inappropriate lawsuits.

[228] Although the categories are not closed, in *Canadian National Railway Co. v. Norsk Pacific Steamship Co.*,[125] the Supreme Court recognized five established categories where recovery for pure economic losses was permitted; namely: (1) negligent misrepresentation; (2) negligence of public authorities; (3) negligent performance of a service; (4) supply of shoddy goods or structures; and (5) relational economic losses. None of these recognized categories is available in the immediate case and thus, once again, there is no compensable harm for the Class Members' negligence causes of action.

[229] Put simply, as pleaded in the Fresh as Amended Statement of Claim, because there are no losses compensable in negligence, it is plain and obvious that the Class Members will not have a certifiable negligence claim or a duty to warn claim.

[230] To elucidate further these points about why there is no viable negligence claim or duty to warn claim in the immediate case, the explanation may begin by noting that pure economic loss is economic loss that is unconnected to physical or mental injury to the plaintiff's person, or to physical damage to property.[126] In the immediate case, the overwhelming majority of the Class Members will have suffered only the threat of pure economic losses and only a few may have suffered actual pure economic losses from identify theft and fraud or from expending money to respond to the threat of a fraud occurring.

[231] In *Maple Leaf Foods,* in a majority decision written by Justice Brown and Martin,[127] the Supreme Court dismissed a negligence claim in a proposed class action by Mr. Submarine franchisees, whose supply chain for sandwich meats was disrupted for several months when the defendant Maple Leaf Foods, the franchisor's supplier, recalled its goods because of a listeria outbreak at its processing plant. The facts of *Maple Leaf Foods* are obviously far different from the immediate case. but the case demonstrates that the legal policy of the law of negligence is that

---

[123] *Carter v. Ford Motor Company of Canada*, 2021 ONSC 4138; *1688782 Ontario Inc. v. Maple Leaf Foods Inc.*, 2020 SCC 35; *Arora v. Whirlpool Canada LP*, 2012 ONSC 4642, affd. 2013 ONCA 657; *Winnipeg Condominium Corp No 36 v. Bird Construction Co*., [1995] 1 S.C.R. 85.
[124] 2000 SCC 60 (McLachlin C.J. and Gonthier, Iacobucci, Major, Bastarache, Binnie and Arbour JJ.).
[125] [1992] 1 S.C.R. 1021.
[126] 1688782 *Ontario Inc. v. Maple Leaf Foods Inc.*, 2020 SCC 35 at para. 17; *Martel Building Ltd. v. Canada*, 2000 SCC 60 at para. 34.
[127] Abella, Moldaver, Côté, and Rowe, JJ. concurring with Justice Brown. Justice Karakatsanis wrote the dissent for herself and Wagner C.J., Martin and Kasirer JJ.

with a few exceptions that can be justified on public policy grounds, tort law leaves pure economic losses to be addressed by the law of contract.

[232] In *Maple Leaf Foods*, in their explanation of the law, Justice Brown and Martin confirmed the rule from *Atlantic Lottery Corp. Inc. v. Babstock*,[128] that negligence law does not recognize the risk of injury or harm or the increased risk of harm or injury as a compensable type of damages and explained that the liability rule from *Winnipeg Condominium Corp No 36 v. Bird Construction Co.*,[129] which would compensate a person for the pure economic loss of repairing defective goods that have not caused any physical harm, was only rationalizable with the general legal principle that there is no compensation for damages that have not yet occurred by recognizing a legal right not to suffer damages from the exposure to an imminent and serious threat to a person's person or property. Justices Brown and Martin noted that the liability rule in *Winnipeg Condominium* protects a right to be free of a negligently-caused real and substantial danger. In other words, it is a predicate for recovery for the pure economic loss that the goods present an imminent real and substantial danger to health and safety. In the immediate case, there is no imminent real and substantial danger to the health and safety of the six million Canadians exposed to the data breach.

[233] The point to emphasize is that an overwhelming majority of the Class Members will not have any losses not even a pure economic loss and for those that suffer a pure economic loss, those losses are not compensable in negligence but by breach of contract and thus it is plain and obvious that as pleaded in the Fresh as Amended Statement of Claim, there is no viable negligence or breach of a duty to warn cause of action.

[234] The above analysis based on decided case law is sufficient to strike out the negligence and breach of the duty to warn claim in the immediate case as against both Capital One and Amazon Web, but I shall continue the analysis by treating the case as a negligence and a breach of a duty to warn case of first instance and I shall determine based on the established principles of the law of negligence whether Amazon Web has a duty of care to the Class Members. In the immediate case, Amazon Web argued that it is plain and obvious that: (a) there was no foreseeability of harm from its pleaded misconduct; (b) it did not have a sufficiently proximate relationship to establish a duty of care; and, (c) there are policy reasons that would negate any duty of care to these Class Members. (Capital One did not make a similar argument.)

[235] The analysis of whether Amazon Web has a duty of care relationship with the putative Class Members may begin by noting that there is no contractual relationship or direct relationship between Amazon Web and the putative Class Members. It is pleaded that the Class Members did not even know that their personal information was being stored on Amazon Web's servers.

[236] Negligence law is based on the existence of a duty of care relationship. The Canadian approach to determining whether there is a duty of care has been developed in a series of Supreme Court of Canada decisions[130] adapting and explaining the House of Lord's decision in *Anns v.*

---

[128] 2020 SCC 19 at para. 33
[129] [1995] 1 S.C.R. 85.
[130] *Haig v. Bamford*, [1976] 1 S.C.R. 466; *Kamloops (City) v. Nielsen*, [1984] 2 S.C.R. 2; *Rothfield v. Manolakos*, [1989] 2 S.C.R. 1259; *Canadian National Railway Co. v. Norsk Pacific Steamship Co*., [1992] 1 S.C.R. 1021; *Hercules Managements Ltd. v. Ernst & Young*, [1997] 2 S.C.R. 165; *Bow Valley Husky (Bermuda) Ltd. v. Saint John Shipbuilding Ltd*., [1997] 3 S.C.R. 1210; *Ingles v. Tutkaluk*, 2000 SCC 12; *Martel Building Ltd. v. Canada*, 2000 SCC 60; *Cooper v. Hobart*, 2001 SCC 79; *Edwards v. Law Society of Upper Canada*, 2001 SCC 80; *Odhavji Estate v. Woodhouse*, 2003 SCC 69; *Childs v. Desormeaux*, 2006 SCC 18; *Syl Apps Secure Treatment Centre v. D. (B.)*, 2007 SCC 38; *Hill v. Hamilton-Wentworth Regional Police Services Board*, 2007 SCC 41; *Design Services Ltd. v. Canada*,

Merton London Borough Council,[131] and derived from the seminal cases of *Donoghue v. Stevenson*[132] and *Hedley Byrne & Co. Ltd. v. Heller & Partners Ltd.*[133]

[237] The categories of negligence are not closed, and if a defendant challenges a plaintiff's cause of action in negligence as legally untenable, the plaintiff needs to show that: (a) the material facts of the pleaded cause of action are within an established category of duty of care; or (b) the material facts of the pleaded cause of action establish a duty of care relationship in accordance with a duty of care analysis.

[238] If a negligence case does not come within an established category, it is necessary to undertake a duty of care analysis. To determine whether a duty of care exists involves satisfying a three-step analysis; *i.e.* (1) foreseeability, in the sense that the defendant ought to have contemplated that the plaintiff would be affected by the defendant's conduct; (2) sufficient proximity, in the sense that the relationship between the plaintiff and the defendant is sufficiently close *prima facie* to give rise to a duty of care; and (3) the absence of overriding policy considerations that would negate any *prima facie* duty established by foreseeability and proximity. Thus, in a new category of case, whether a relationship giving rise to a duty of care exists depends on foreseeability, moderated by policy concerns.[134]

[239] To determine the foreseeability element, the court asks whether the harm that occurred was the reasonably foreseeable consequence of the defendant's negligence.[135]

[240] A reasonable foreseeability analysis requires only that the general harm, not its manner of incidence, be reasonably foreseeable.[136] The foreseeability element was examined by the Supreme Court of Canada in *Rankin (Rankin's Garage & Sales) v. J.J.*,[137] where the Court reversed the conclusion of the lower courts that a garage owner had a duty of care to a person injured following the theft of the vehicle from the garage. A majority of the court concluded that for liability, the defendant ought to have foreseen the type of harm actually suffered. Justice Karakatsanis for the majority said that the proper question to ask is whether the plaintiff has offered facts to persuade the court that the risk of type of damage that occurred was reasonably foreseeable to the class of plaintiff that was damaged.[138] She said that there must be a connection between the defendant's wrong and the injury suffered by the plaintiff.

[241] In the immediate case, the wrong suffered by the Class Members is that there was a data breach perpetrated by Ms. Thompson. In the immediate case, that wrong is not connected to a wrong perpetrated by Amazon Web to the Class Members. Like the garage owner defendant in *Rankin (Rankin's Garage & Sales) v. J.J.*, who could have foreseen the possibility of the vehicle

---

2008 SCC 22; *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27; *Fullowka v. Pinkerton's of Canada Ltd*., 2010 SCC 5; *R. v. Imperial Tobacco Canada Ltd.*, 2011 SCC 42; *Saadati v. Moorhead*, 2017 SCC 28; *Deloitte & Touche v. Livent Inc. (Receiver of)*, 2017 SCC 63; *Rankin (Rankin's Garage & Sales) v. J.J*., 2018 SCC 19.

[131] [1978] A.C. 728 (H.L.).

[132] [1932] A.C. 562 (H.L.).

[133] [1964] A.C. 465 (H.L.).

[134] *Anns v. Merton London Borough Council*, [1978] A.C. 728 (H.L.)*; Mustapha v. Culligan of Canada Ltd.* 2008 SCC 27 at para. 4.

[135] *Deloitte & Touche v. Livent Inc. (Receiver of)*, 2017 SCC 63 at paras. 33-35; *Cooper v. Hobart*, 2001 SCC 79 at para. 30; *Donoghue v. Stevenson*, [1932] A.C. 562 at p. 580 (H.L.).

[136] *Bingley v. Morrison Fuels, a Division of 503373 Ontario Ltd.*, 2009 ONCA 319 at para. 24.

[137] 2018 SCC 19 (Justice Karakatsanis with Chief Justice McLachlin, Justices Abella, Moldaver, Wagner, Côté and Rowe concurring; Justices Brown and Gascon dissenting).

[138] *Rankin (Rankin's Garage & Sales) v. J.J.*, 2018 SCC 19 at para. 24.

it was repairing being stolen and misused, Amazon Web could have foreseen the possibility of data it was storing being stolen and misused, but that does not make the harm that occurred a reasonably foreseeable consequence of Amazon Web's alleged carelessness.

[242] Where the Class Members' duty of care argument runs further aground is on the matter of proximity. Proximity focuses on the type of relationship between the plaintiff and defendant and asks whether this relationship is sufficiently close that the defendant may reasonably be said to owe the plaintiff a duty to take care not to injure him or her.[139]

[243] Proximate relationships giving rise to a duty of care are of such a nature that the defendant in conducting his or her affairs may be said to be under an obligation to be mindful of the plaintiff's legitimate interests.[140] The proximity inquiry probes whether it would be unjust or unfair to hold the defendant subject to a duty of care having regard to the nature of the relationship between the defendant and the plaintiff.[141] The focus of the probe is on the nature of the relationship between victim and alleged wrongdoer and the question is whether the relationship is one where the imposition of legal liability for the wrongdoer's actions would be appropriate.[142] Proximity focuses on the connection between the defendant's undertaking, the breach of which is the wrongful act, and the loss claimed.[143] The proximity analysis involves considering factors such as expectations, representations, reliance, and property or other interests involved.[144] Proximity is not concerned with how intimate the plaintiff and defendant were, or with their physical proximity, so much as with whether the actions of the alleged wrongdoer have a close or direct effect on the victim, such that the wrongdoer ought to have had the victim in mind as a person potentially harmed.[145] The proximity analysis is intended to be sufficiently flexible to capture all relevant circumstances that might in any given case go to seeking out the close and direct relationship that is the hallmark of the common law duty of care.[146]

[244] In the immediate case, it is plain and obvious that the Class Members would have no expectations *vis à vis* Amazon Web, which was unknown to the Class Members. Amazon Web made no representations or undertook no responsibilities to the Class Members. Amazon Web's responsibilities were to Capital One, which was not the agent for the Class Members.

[245] It is not so much that there was not a proximate relationship between the Class Members and Amazon Web. In the immediate case, there was no relationship upon which proximity could be established. The Class Members and Amazon Web were not in a proximate relationship. They had no relationship at all. Amazon Web's relationship was with Capital One and any undertaking by Amazon Web would have been provided to Capital One in the context of a contractual relationship. Any reliance on Amazon Web's undertaking could only have been by Capital One, since the Class Members were unaware that the data they provided to Capital One was stored with

---

[139] *Donoghue v. Stevenson,* [1932] A.C. 562 (H.L.); *Eliopoulos v. Ontario (Minister of Health & Long-Term Care)* (2006), 82 OR (3d) 321 (CA), leave to appeal to SCC ref'd [2006] SCCA No 514.
[140] *Odhavji Estate v. Woodhouse,* 2003 SCC 69 at para. 49; *Hercules Managements Ltd. v. Ernst & Young*, [1997] 2 SCR 165 at para. 24.
[141] *Syl Apps Secure Treatment Centre v. D. (B.),* 2007 SCC 38 at para. 26.
[142] *Hill v. Hamilton-Wentworth Regional Police Services Board,* 2007 SCC 41 at para. 23.
[143] *Deloitte & Touche v. Livent Inc. (Receiver of),* 2017 SCC 63.
[144] *Cooper v. Hobart,* 2001 SCC 79 at para. 34; *Hill v. Hamilton-Wentworth Regional Police Services Board*, 2007 SCC 41 at para. 23; *Odhavji Estate v. Woodhouse*, 2003 SCC 69 at para. 50.
[145] *Hill v. Hamilton-Wentworth Regional Police Services Board,* 2007 SCC 41 at para. 29.
[146] *Saadati v. Moorhead*, 2017 SCC 28 at para. 24.

Amazon Web.

[246] Moving on in the duty of care analysis, if the plaintiff establishes a *prima facie* duty of care, the evidentiary burden of showing countervailing policy considerations shifts to the defendant, following the general rule that the party asserting a point should be required to establish it.[147] Policy concerns raised against imposing a duty of care must be more than speculative, and a real potential for negative consequences must be apparent.[148]

[247] The final stage of the analysis is not concerned with the type of relationship between the plaintiff and the defendant. At this stage of the analysis, the question to be asked is whether there exist broad policy considerations that would make the imposition of a duty of care unwise, despite the fact that harm was a reasonably foreseeable consequence of the conduct in question and there was a sufficient degree of proximity between the plaintiff and the defendant such that the imposition of a duty would be fair.[149] The final stage of the analysis is about the effect of recognizing a duty of care on other legal obligations, the legal system and society more generally.[150]

[248] In the English case of *Caparo Industries plc v. Dickman*,[151] the House of Lords delineated public policy reasons for negating a *prima facie* duty of care; namely: (a) whether the imposition of liability would be fair having regard to the defendant's control over the risk of harm to the plaintiff; (b) whether the imposition of liability is disproportionate to the gravity of the wrong; (c) whether the imposition of liability would entail indeterminate liability in the sense that nature, duration, and number of claims could not be realistically predicted or determined; (d) whether the imposition of liability would flood the court with claims; (e) whether the imposition of liability would introduce a wide area of claims; (f) whether the imposition of liability would encourage defensive practices; i.e., socially undesirable behaviour modification; (g) whether the plaintiff had alternative remedies to a lawsuit; (h) whether the imposition of liability would disturb the contractual allocation of risk; and (i) whether the imposition of liability would adversely affect international trade or comity between nations.

[249] In the immediate case, it is plain and obvious that if Amazon Web had a *prima facie* duty of care to the Class Members, it would be negated by any or all of the circumstances that the imposition of liability would: (a) entail indeterminate liability; (b) flood the court with claims; (c) introduce a wide area of claims; and (d) disturb the contractual allocation of risk.

[250] I therefore conclude that it is plain and obvious that there is no viable negligence or duty to warn claim in the circumstances of the immediate case as against Amazon Web.

[251] For all these reasons, I strike the negligence claim and the duty to warn claim without leave to amend.

P. Breach of Contract/Negligent Breach of Contract

[252] The elements of a cause of action for breach of contract, which is a strict liability regime

---

[147] *Childs v. Desormeaux*, 2006 SCC 18 at para. 13.
[148] *Hill v. Hamilton-Wentworth Regional Police Services Board*, 2007 SCC 41 at paras. 47-48; *Fullowka v. Pinkerton's of Canada Ltd.*, 2010 SCC 5 at para. 57.
[149] *Cooper v. Hobart*, 2001 SCC 79 at para. 37; *Odhavji Estate v. Woodhouse*, 2003 SCC 69 at para. 51.
[150] *Cooper v. Hobart*, 2001 SCC 79 at para. 37; *Odhavji Estate v. Woodhouse*, 2003 SCC 69 at para. 51.
[151] [1990] 2 AC 605 (H.L.)

actionable without proof of damages, [152] are: (1) the plaintiff and the defendant are parties to a validly formed contract; and, (2) the defendant fails to perform his or her obligations under the contract.[153]

[253] The Plaintiffs plead breach of contract and negligent breach of contract as against Capital One and Amazon Web.[154] The alleged breach of contract is the failure to return or to destroy the personal information after the single purpose use was spent. However, the claims are not class-wide claims, and the Plaintiffs' factums and Class Counsel's oral submissions reveal that the contract claims are ancillary or incidental or supplementary to the main thrust and purpose of the Plaintiffs' action.

[254] The Fresh as Amended Statement of Claim does not ever plead a straightforward breach of contract claim for the failure to honour Capital One's promises about compliance with its own privacy policies. The breach of contract pleading is the alternative qualified (if/then) allegation in paragraph 121 that:

> In the alternative, if a contract existed between Capital One and any of the Class Plaintiffs, [then] Capital One was in breach of contract and in negligent breach of contract in maintaining, storing and using the Confidential Data after the Single Purpose Use was spent.

[255] The Fresh as Amended Statement of Claim appears to purposefully avoid a straightforward breach of contract claim applicable to all of the Class Members who applied for a Capital One credit card.

[256] An analysis of the Fresh as Amended Statement of Claim, the deconstruction of Class Counsel's legal logarithm, discussed in the next part of these Reasons for Decision, and the kerfuffle that marred the start of Phase I of this certification hearing reveals that Class Counsel's actual purpose is to negate the contractual force of the application form by which Capital One collected the personal information, the contract document that is the genuine beginning of the factual narrative that led to the data breach.

[257] The Plaintiffs could have but they assiduously avoid pleading a straightforward breach of contract claim against Capital One based on the application form. In the immediate case, the Plaintiffs might have pled a straightforward breach of contract alleging that Capital One breached its contractual promises to keep the Class Members' personal information secure and its promise to comply with Canadian privacy laws such of PIPEDA. Breach of contract entails at least nominal damages for all Class Members and some Class Members would have actually suffered economic losses from Capital One's breach of contract.

[258] In a "smoke em if you got em"-argument instead of a straightforward breach of contract claim for the whole class, the Plaintiffs plead a negligent breach of contract for the Class Members who have credit card agreements with Capital One. This pleading is a doctrinal fantasy. The failure to perform a contract promise be it intentional, reckless, careless, or because of matters beyond the control of the promisor is irrelevant to a breach of contract claim. Negligent performance of a contract is a legally meaningless concept to a cause of action for breach of contract, which is about

---

[152] *Fraser Park South Estates Ltd v. Lang Michener Lawrence & Shaw*, 2001 BCCA 9 at para. 46, leave to appeal to SCC refused [2001] S.C.C.A. No. 72.

[153] *Adams-Smith v. Christian Horizons*, [1997] O.J. No. 2887 (Gen. Div.).

[154] Fresh as Amended Statement of Claim paragraphs 1(c), 1(e), 4, 11, 21, 54, 69, 70, 72, 73, 74, 77, 81, 82, 84, 87, 100, 106, 114, 116, 117, 118, 121, 128, 133.

what are the contract promises and whether those promises have been performed,[155] not about what motivated or caused the contract to be breached.

[259] I conclude that although the Plaintiffs could have advanced a certifiable breach of contract claim for the whole class, they have not done so. I conclude that the Plaintiffs do not satisfy the cause of action criterion for a claim for breach of contract. The question then is whether I should grant leave to the Plaintiffs to deliver a Second Fresh as Amended Statement of Claim. However, for the reasons expressed above and for the reasons expressed next in Part Q, no purpose would be served in granting leave, and I decline to do so. In the result, I do not certify the pleaded breach of contract claim.

Q. Legal Theories, and Legal Logarithms

[260] In this next to the last part of my Reasons for Decision, I explain the third reason why the Plaintiffs' Fresh as Amended Statement of Claim should be struck without leave to amend. This brings me to the matter of Class Counsel's Compendium, which was filed on the weekend before the start of Phase I of the certification motion. I have attached the flow chart from the compendium as Schedule "B" to these Reasons for Decision.

[261] The 56-page compendium was filed to supplement the Plaintiffs' factums and to explain Class Counsels' theory of the case for Phase I of the certification motion. In this part of my Reasons for Decision, I shall deconstruct the compendium, which I have labelled a legal logarithm, because Class Counsel submitted that it covers every conceivable factual variable and would inevitably lead to a successful outcome for the Class Members. I shall explain why all that Class Counsel achieved is a third reason to strike the Fresh as Amended Statement of Claim.

[262] An analysis of the compendium, which sets out Class Counsel's theory of the immediate case, which Class Counsel described as a ladder of liability, reveals that by design it is a "tails I win, heads you lose" legal logarithm. On the first rung of the ladder, the theory is that once Capital One granted or refused to grant a credit card, any further use of the Class Members' personal information from the application for the credit card was an intrusion on seclusion, a misappropriation of personality, a conversion, a breach of confidence, negligence, a breach of a duty to warn, a breach of trust and fiduciary duty, and conduct warranting strict liability.

[263] In oral argument, Mr. Elliott stated that although the Plaintiffs had pleaded negligent breach of contract, this pleading was just a complement or supplement to the Plaintiffs' negligence claim. In other words, the Plaintiffs acknowledged that for those Class Members who had contracts, the standard of care would be measured by the standard of contract performance not by negligence standards. In reply argument, however, Mr. Campion asserted that the Class Members were advancing breach of contract claims at least against Capital One.

[264] The theory of the Plaintiffs' case continued on another rung of the ladder, that if the contracts entered into by the Class Members authorized other uses or future uses of the personal information apart from its use to apply for credit, then there was no lawful consent to those other uses, and, thus, the other uses which occurred when Capital One merchandized the personal information or exported it to the United States to be aggregated with American citizens' personal information, there was a breach of confidence, a conversion, a breach of trust and fiduciary duty,

---

[155] *Rotary Drum Corp. v. Louisiana-Pacific Canada Ltd*., 2001 ABQB 297; *Adams v. Thompson, Berwick, Pratt & Partners*, (1986) 1 BCLR (2d) 97 (S.C.).

and conduct warranting strict liability. In addition, once again, Capital One was liable for intrusion on seclusion, a misappropriation of personality, a conversion, a breach of confidence, negligence, a breach of a duty to warn, a breach of trust and fiduciary duty, and conduct warranting strict liability.

[265] Further, the theory of the Plaintiffs' case was that if the contracts entered into by the Class Members did authorize other uses or future uses of the personal information apart from its use to apply for credit, then that authorization lapsed when the risk of the misuse of the confidential information was substantially increased by its exportation to the United States, where its aggregation with American citizens' personal information was an irresistible attraction for organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties who would inevitably seek to steal this valuable asset.

[266] In oral argument, Class Counsel explained that the numerous statutes including the privacy acts of various provinces which had been pleaded were relevant to the theory of the case not so much because they were actionable, which they might be, but for a different reason. The relevance of these statutes was that the Defendants had admitted that they were bound by Canadian law. Thus, the Defendants' breaches of PIPEDA and other privacy statutes established the elements of the intentional conduct that were prerequisites to intrusion on seclusion, conversion, and strict liability and these breaches were also contract breaches for those Class Members who had contracts.

[267] Given the difference in proximity between the Class Members and Amazon Web, one might think that the Plaintiffs would need a different theory of the case as against Amazon Web. However, they advanced the same case against Amazon Web and the essence of the argument is that Amazon Web was party or partner or complicit in the misconduct of Capital One and also vicariously liable for Ms. Thompson's misdeeds since they trained her and provided her with the opportunity to learn of the defects in their data storage technology and in the lacking security safeguards in Capital One's contract with Amazon Web.

[268] Apart from the situation that the Plaintiffs' 55-page Fresh as Amended Statement of Claim egregiously contravenes the rules of pleading and apart from the situation that the pleading needs a 58-page compendium as an operator's manual, upon analysis, Class Counsel's legal theory implodes, explodes, and crumbles.

[269] In the immediate case, when I granted Class Counsel carriage of this proposed class action, it appeared that they were posed to advance the causes of action for a data breach incident that occurred into 2019. As revealed by their Facta, the Compendium, and oral argument, Class Counsel have proudly transformed a $10.9 billion data breach case about a single incident into a still ongoing $240 billion misappropriation and misuse of data case about the gathering of data for three decades in the United States and over one decade in Canada. Class Counsel have changed a data breach case into a case about whether a commercial actor that has gathered personal information can be liable for breach of privacy if the commercial actor, in this case a bank, subsequently uses the information beyond the consents that it obtained when it gathered the information.

[270] Class Counsel's legal theory, however, implodes when one reads the contract documents that are incorporated by reference into the Fresh as Amended Statement of Claim and that normally would have been produced for a certification motion without acrimonious incident. Class

Counsel's legal theory, however, explodes when one analyzes each of the pleaded causes of action, as I have done in Parts H to P of these Reasons for Decision. As admirable as Class Counsel's intellectual effort to design a legal prediction machine might be, cases are decided with law applied to proven facts. Causes of action are not custom made, and lawsuits are not decided by a tautological legal logarithm. All that Class Counsel achieved by the Compendium is a third reason to strike the Fresh as Amended Statement of Claim.

[271] I emphasize that in their development and prosecution of a data misappropriation and misuse case, the Plaintiffs will have nothing to do with a conventional breach of contract claim for all the Class Members. Although Mr. Campion and Mr. Elliot in their oral submissions could not get on the same page as to the extent to which there as any breach of contract claim involved in the immediate case, it emerged from a deconstruction of the legal logarithm, that Class Counsel have rejected a straightforward breach of contract approach, and they rather substituted a complex matrix of causes of action, some of which causes of action are advanced not as discrete causes of action but rather as proof of components of other causes of action. The breach of contract claim, such as it is, is subsumed and overwhelmed and displaced by the negligence claim.

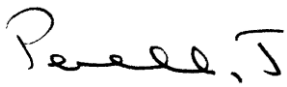
[272] If difficulties in commonality could be overcome, the Plaintiffs might have had a straightforward, reasonably strong, and possibly certifiable data breach case for breach of contract against Capital One for the 2019 data breach. However, Mr. Campion submitted that: (a) some Class Members did not have any contracts with Capital One; (b) if there were any contracts with Class Members, then the contracts were unenforceable or at least any exculpatory provisions in those contrasts were not enforceable pursuant to the common law about unconscionable contracts or pursuant to statutory provisions like consumer protection statutes that would nullify the disclaimers; and (c) the consents to the use of personal information contained in the credit application and in the credit card agreement were illegal, unenforceable, and contrary to PIPEDA and other privacy laws.

[273] It is not for me to speculate why Class Counsel eschewed a straightforward breach of contract case or to speculate how Class Counsel might have pled the Class Members' Statement of Claim to advance other causes of action that are legally viable and properly pleaded. I can, however, conclude that it is plain and obvious that aided by the Compendium, the Fresh as Amended Statement of Claim does not satisfy the cause of action criterion for certification and no purpose would be served by granting leave to deliver a Second Fresh as Amended Statement of Claim.

R. Conclusion and the Matter of Costs

[274] For the above reasons, I dismiss the Plaintiffs' motion to certify this action as a class proceeding. I lift the stay of other proposed class actions that I imposed when I granted carriage to the Plaintiffs' consortium of Class Counsel.

[275] If the parties cannot agree about the matter of costs, they may make submissions in writing beginning with Capital One and Amazon Web's submissions within thirty days of the release of these Reasons for Decision followed by the Plaintiffs' submissions within a further thirty days.



Perell, J.

Released: August 4, 2021.

Schedule "A" – Fresh as Amended Statement of Claim

PART I – PRAYER FOR RELIEF

1. The plaintiffs claim on their own behalf and on behalf of a putative class […]

(a) an order certifying this proceeding as a class proceeding or its equivalent and appointing the plaintiffs representatives of the Class for the purpose of prosecuting a class proceeding against the defendants;

[…]

(c) against each and every defendant, general and special damages, an order for aggregate damages […]and/or, punitive damages, exemplary damages, and moral damages, per plaintiff and for the Class Plaintiffs as a group for: breach of confidence; breach of privacy, intentional and/or reckless conduct leading to intrusion upon seclusion, appropriation of the name and information of the Class Plaintiffs for the advantage of Capital One; negligence, breach of statutory obligations; breach of trust, breach of fiduciary duty; breach of duty to warn; and, alternatively, breach and negligent breach of contract;

(d) an accounting for all profits directly or indirectly earned by each and every defendant and an order requiring each defendant to disgorge such profits;

(e) declarations that the defendants each breached: (i) the relevant Consumer Protection Acts in each provincial and territorial jurisdiction in Canada (listed in Schedule "A"); (ii) the relevant Privacy Acts in each provincial and territorial jurisdiction in Canada (listed in Schedule "A"); (iii) the relevant Negligence Acts in each provincial and territorial jurisdiction in Canada (listed in Schedule "A"); (iv) *Civil Code of Quebec*, L.R.Q., c. C-1991; (v) the *Personal Information and Protection and Electronic Documents Act* RSC, 2000, c.5 ("PIPEDA"); (vi) *the Bank Act* S.C. 1991, c.46; (vii) *Payment Cards Networks* Act, S.C., 2010, c.12; (viii) *Electronic Commerce Act*, 2000, S.O. 2000, c.17; (ix) *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c.F.31, (all of which statutes which are listed in Schedule "A" hereof); and damages arising from each and every breach of statutory obligations;

(f) a mandatory order that the Confidential Data (as hereinafter defined) be returned by Capital One (hereinafter defined to include all Capital One defendants) to each of the Class Plaintiffs (as hereinafter described);

(g) […]

(h) costs of administering any plan of distribution arising from recoveries in this action or such other related orders as this Honourable Court finds appropriate;

(i) prejudgment interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43, s. 128 (and all relevant similar statutes providing for prejudgment interest in every Canadian provincial and territorial jurisdiction – hereinafter listed in Schedule "A" hereof);

(j) post-judgment interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43, s. 29 (and all relevant similar statutes providing for prejudgment interest in every Canadian provincial and territorial jurisdiction – hereinafter listed in Schedule "A" hereof);

(k) costs […]

(l) such further and other relief this Honourable Court seems just.

PART II – THE PARTIES

THE PLAINTIFFS

2. The plaintiff Rina Del Giudice ("Giudice") resides in the Province of Ontario and is a Capital One Canada and Capital One USA (as hereinafter defined) cardholder and a proposed consenting representative plaintiff in this putative class action.

3. The plaintiff Daniel Wood ("Wood") resides in the Province of Alberta and is a Capital One Canada and Capital One USA (as hereinafter defined) cardholder and a proposed consenting representative plaintiff in this putative class action.

CLASS DEFINITION

4. The plaintiffs Giudice and Wood have consented to represent approximately 6 million Canadians, being the putative class plaintiffs ("Class Plaintiffs") described to include: the class of persons in Canada who applied for credit cards between 2005 and 2019 and/or provided confidential financial and personal information (the "Confidential Data") to 'Capital One' (hereinafter defined to include all five Capital One defendants) or contracting parties in Canada, including the Bay, Costco, WalMart, JC Penney and MasterCard, and others unknown to the Class Plaintiffs, (collectively, the "Capital One Partners") between 2005 and 2019.

THE DEFENDANTS

5. The defendants Capital One Financial Corporation ("Capital One Financial"), Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, "CapO-US") are part of a group of companies comprised of Capital One Financial as the parent and the remaining Capital One companies identified in paragraph 6 of this pleading and other corporate entities and/or subsidiaries unknown to the Class Plaintiffs at this time, which are directly or indirectly owned and/or controlled by Capital One Financial (entities collectively and individually hereinafter referred to as "Capital One"). The Class Plaintiffs are not presently aware of the full details of the corporate structure, subsidiary and entity structure and reporting responsibilities involving data gathering commitments, preservation, security, transfer, confidentiality and mishandling breaches and related corporate issues of the individual corporate and entity members comprising Capital One, relevant to this proceeding.

6. The defendants Capital One Bank (Canada Branch), Capital One (Services) Canada Inc., (collectively for the Canadian entities alone, "CapO-Canada" and collectively with the USA entities, "Capital One") are directly or indirectly wholly owned and/or controlled subsidiaries or entities of Capital One Financial.

7. The defendants Amazon Web Services (Canada) Inc. ("Amazon Canada") and Amazon Web Services Inc. ("Amazon USA") (collectively, "Amazon Web") are, *inter alia*, in the business of making profits from global data centres for storing and protecting data received from third party contractors, in this case Capital One.

8. The defendant GitHub, Inc. ("GitHub") is a corporation incorporated in carrying on the business of building and controlling software platforms permitting webhosting and allowing users to manage and store computer information and permitting the subsequent public access to data and other digital information placed on the platforms.

9. The defendant Paige A. Thompson ("Thompson") is, *inter alia*, a computer systems engineer residing in the United States of America, also known on the internet as "ERRATIC" and a former employee, by contract and by operation of law, of Amazon Web and/or Capital One.

PART III – THE FACTS

Introduction

10. CapO-US began its modern business in the United States of America (USA) in 1994 as a regional (non-bank) financial institution focusing, inter alia, on consumer credit including credit cards. This action involves, *inter alia*, a review of the growth and conduct of Capital One first in the USA as a significant context to the data breach in or about March 2019 (the "Data Breach") complained of in this case, and second internationally, with particular reference to Canada from 1994 to date. The Data Breach involves the Confidential Data (as hereinafter defined) of 6 million Class Plaintiffs (as hereinafter defined) delivered in trust to CapO-Canada for a Single Purpose Use (as hereinafter defined) and (unknown to the Class Plaintiffs) as migrated to the USA and aggregated with the Confidential Data of a further group of 94 million other applicants who sent their Confidential Data to CapO-US (collectively for the purpose of applying for a Capital One credit card). The Confidential Data of the Class Plaintiffs, as hereinafter defined, unknown to the Class Plaintiffs, was retained past the time of the Single Purpose Use (as hereinafter defined) being spent; and wrongly: stored for use on servers in Canada; migrated for storage and use to servers in the USA; aggregated with data of the other 94 million applicants to create a database of 100 million bank applicants; migrated for storage and use from the servers of Capital One to the servers of Amazon Web; and subsequently made the subject of the (unknown to the Class Plaintiffs) inevitable Data Breach and unrestricted publication to the world. The Data Breach caused damages to each Class Plaintiff, required at a minimum to protect the Confidential Information from the residual risk of harm to their Data, over time, of being potentially and/or actually exposed to and improperly used by organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties ("Data Abusers").

11. The five Capital One defendants, defined as "Capital One", variously committed the torts of: (i) conversion, intentional intrusion upon seclusion, reckless intrusion upon seclusion, intentional misappropriation of Financial Personality (as hereinafter defined), reckless misappropriation of Financial Personality, and breach of a duty to warn (collectively, the "Breach of Privacy Rights"); (ii) breach of trust and breach of fiduciary duty (collectively "Breach of Banking Trust"); (iii) negligence ("Negligence"); and, alternatively, (iv) breach of contract and negligent breach of contract (if a contract existed at all), (collectively, "Negligent Breach of Contract"). Amazon Web committed the torts of: Breach of Privacy Rights, Negligence, and Negligent Breach of Contract. GitHub committed the torts of Breach of Privacy Rights and Negligence. Thompson committed the torts of Breach of Privacy Rights, Negligence, and Negligent Breach of Contract.

12. The relevant conduct of the defendant is pleaded in three different decades: (i) Decade 1 – 1994 to 2005; (ii) Decade 2 – 2005 to 2015; (iii) Decade 3 – 2015 to 2020, and following.

Decade 1 – 1994 to 2005

13. During this decade CapO-US was and became an industry leader in the use of data. It developed the information based strategy ("IBS Strategy") whereby it was involved in customizing credit card solutions to consumers, product innovation, marketing and risk management and essentials of success in consumer financial services. The IBS Strategy was the basis which allowed Capital One to compete against all existing issuers of credit cards and to alter the entire structure of consumer credit, first in the USA and secondly in Canada beginning in Decade 2.

14. Using data and technology and the IBS Strategy, CapO-US successfully competed with all competitors in the credit card field by rejecting the "one size fits all" credit card model to tailoring a credit card for each applicant who was eligible or decided to become a customer of Capital One.

15. During Decade 1, the American financial institution industry was ripe for change. The industry was facing an ever-more sophisticated technological, computer and data revolution (the "Computer and Data Revolution"). The revolution continued and caused exponential and ever-increasing changes in, *inter alia*, to the financial institution industry up to today's date.

16. As Decade 1 matured, CapO-US saw itself then as a digital leader. It used its technological vision to disrupt the existing banking industry by, *inter alia*, recognizing that banking was inherently a digital product. It conceived that the most competitive banks would become world class software, digital and information companies. CapO-US deeply embedded technology, design, software development and significantly data into every aspect of its enterprise establishing the foundational underpinnings of this digital company, including the aggressive use of data of every applicant and customer who submitted Confidential Data (as hereinafter defined) as if CapO-US had a proprietary interest in the asset represented by the Confidential Data.

17. As early as 1994, CapO-US recognized and exploited data farmed from credit card applicants and customers alike a major business asset owned by them. CapO-US and in Decades 2 and 3 CapO-Canada continued to exploit the data of applicants and their customers as a Capital One asset for the three decades in question. The ever-increasing importance of data was, *inter alia*, used to: (i) assess the credit worthiness of the applicants; (ii) monitor credit worthiness of customers; (iii) develop and assess their existing and potential customer base and the needs of its existing and potential customer base; and (iv) otherwise use and sell the data as a credit design tool, market analysis base, internal asset, and external asset to sell to third parties concerned about customer behaviour. CapO-US, and in Decades 2 and 3, CapO-Canada, used the data collected by American financial institutions and, later, Canadian and American banking applicants and customers to expand their business enterprise, impose market dominance in the consumer credit business, and to reap consistent and increasing annual profits over the years in question.

18. In Decade 1, in executing the business derived from the IBS Strategy, CapO-US retained, stored, used, misused and profited from the data collected from, inter alia, each and every applicant who applied for a credit card. The personal and financial data collected for each applicant included the individual or business information as follows: the Social Insurance Number ("SIN"), their bank account numbers, credit history, names, addresses, and dates of birth ("Confidential Data"). CapO-US invited applicants to share Confidential Data for the single purpose of assessing credit worthiness and eligibility for a credit card (the "Single Purpose Use"). Capital One did not have the legal right to use the Confidential Data for any other purpose. CapO-US retained the Data after the Single Purpose Use was spent, stored the Confidential Data on their own servers, internally and externally used the Data for business planning and profit, exposed the Data to ever-increasing risk of a data breach and failed to warn any of the applicants and customers of the increasing risk to them of a data breach that would inevitably cause each applicant and customer damage if and when the inevitable (on the facts of this case) data breach was attempted and successful.

19. During Decades 1, 2 and 3, Capital One built infrastructure and capabilities of a technological company through iterative software development, modern computer architecture to accelerate innovation, use of open source and cloud technology as it became available and re-inventing internal processes, operations and governance to ensure its agility in the marketplace. In the early first decade, this technology enabled CapO-US to design its IBS Strategy permitting it to 'mass customize' its credit card offerings, producing the right product for the right customer at the right time and for an individualized price. In so doing, Capital One used its data collected and analytics to solve big problems that were not an afterthought, but part of the DNA of its enterprise so that it permeated every aspect of the business. Capital One leveraged the data it collected to pursue data usage opportunities which added greatly to its strategy, marketing, research and programme development, allowing it to transition from aggressively competitive to a world leader in consumer credit and credit cards.

20. Over Decade 1, and later for the Confidential Data of the Class Plaintiffs in Decades 2 and 3, the gathering, possession, retention, storage, migration, use and sale for profits and misuse for profits and threats to personal and financial data received from their applicants and customers by CapO-US became increasingly important, profitable and under threat (as hereinafter set out).

21. The dark seeds of the Breach of Privacy, Breach of Banking Trust, negligence and, alternatively, negligent breach of contract and other laws regarding the use of Confidential Data by CapO-US and later CapO-Canada was the surreptitious and persistent retention, storage, migration, internal use

and external use of the Confidential Data beyond the Single Purpose Use and indefinitely, for profit, as if the Data were an asset owned by Capital One.

22. By the end of the first decade, CapO-US had developed a diversified portfolio of financial services related broadly to consumer credit, including credit cards, automobile loans and home equity loans serving at least 48.6-million customers. CapO-US had managed loans outstanding in the amount of $80-billion, and net income of $1.543-billion. It had become a Fortune 200 company, and consistent with its competitive strategy developed innovative marketing programmes across the USA that allowed it to become one of the most recognizable brands in the USA. It had stated goals of stability and flexibility, investment and growth and a desire to drive down costs.

23. Two new horizons beckoned CapO-US: (1) institutional; and (2) geographic. Firstly, CapO-US had long desired to become a bank in the USA. By the end of the first decade, CapO-US had been approved to become a Bank Holding Company by the Federal Reserve Board of the USA. Secondly, CapO-US decided to further expand and compete in larger international markets. For the purposes of this action, the new geographic market was Canada. CapO-US planned a major international business outreach in Canada sometime in the latter part of Decade 1 (the "Canada Campaign").

24. During Decade 1 and continuing into Decades 2 and 3, CapO-US began its detailed planning, analysis, institutional changes and corporate decisions to bring into effect the Canada Campaign (the exact dates of which are unknown to the Class Plaintiffs). CapO-US created the details of the Canada Campaign, as detailed in reports analyzing, reviewing, effecting and continuing the Campaign based on, inter alia, marketing, strategy, data technology, structural, legal, risk, profit expectation, financial reports on credit, consumer credit, credit card, automobile loans, home equity loans prepared prior to the commencement of the Canada Campaign. The reports detailed, inter alia, the goals, target consumers, banking structure, Canadian privacy laws and standards, prospects of profitability, and other related issues.

25. As Decade 1 came to a close, CapO-US had perfected its marketing strategy in the USA, including its use of Confidential Data. The IBS Strategy upon which data use was based was adopted into the Canada Campaign and largely, if not entirely, directed from the executive offices of CapO-US (the "CapO Data Strategy"). CapO-US was now prepared to embark upon its further geographic and banking expansion during its second decade, including and, particularly in this action, the Canada Campaign.

Decade 2 – 2005 to 2015

Introduction

26. To effect the Canada Campaign, CapO-US incorporated wholly owned subsidiaries in Canada (CapO-Canada), including a bank branch [Capital One Bank (Canada Branch)] incorporated under the Federal *Bank Act* in 2005. CapO-Canada (the two Canadian corporate defendants) were created and remained as wholly owned subsidiaries fully controlled by CapO-US, with limited local discretion over the consumer credit business, including credit cards and the collection of Confidential Data and its unauthorized use after the Single Purpose Use was spent, applying the tenets of the CapO Data Strategy.

27. In Decade 2, CapO-US continued to apply the CapO Data Strategy, relying upon the IBS Strategy involving technology, consumer credit (including credit cards), and data farming, making it highly successful and profitable in the USA, and as Decade 2 developed in Canada. CapO-US adopted the same business model into Canada, particularly regarding its use of the Confidential Data received from applicants in Canada who responded to the CapO-Canada marketing campaign which was part of the Canada Campaign.

28. The adoption of the CapO Data Strategy into Canada failed to take into proper account the banking, privacy, consumer protection laws, legislation, regulation, regulatory movings, court decisions and data protection standards extant in Canada throughout Decades 1, 2 and 3 (the "Data

Protection Laws and Standards"). The relevant material facts arising in Decade 2 regarding the impugned conduct of all five corporations, namely Capital One are hereinafter organized as follows: (a) impact of banking and the Canada Campaign; (b) Confidential Data – collection and permitted analysis and Single Purpose Use; (c) Confidential Data – retention, storage, migration to the USA and increasing risk; and (d) Confidential Data – use and misuse for profit by Capital One.

(a) *Impact of Banking and the Canada Campaign*

29. At the commencement of the second decade, CapO-US fulfilled its long-held desire to become a bank holding company when it acquired an operating bank in the USA called Hibernia. The acquisition of the USA bank increased CapO-US' and Capital One's managed loans to $106-billion. Capital One's business in the USA now developed beyond consumer credit, credit cards, auto loans, home equity loans and data into a banking enterprise with all of the new and unfamiliar obligations of their trust and fiduciary obligations owed to their applicants and customers who delivered Confidential Data (as the assets of the applicants and customers).

30. In this new and novel banking context (for Capital One), assets received by them as a bank from their potential and/or actual customers were not and never became the property of Capital One and could never properly be used internally and externally, retained, stored, migrated or sold. The Confidential Data received from the Class Plaintiffs in Canada by CapO-Canada and/or CapO-US represented exclusive assets of the Class Plaintiffs received temporarily and held by the banks only for the Single Use Purpose. Past the completion of the Single Use Purpose, any retention, storage, migration, internal use, external use, or other dealing of the assets was a breach of trust and fiduciary duty owed by CapO-Canada and/or Capital One to the Class Plaintiffs.

31. As part of the Canada Campaign, CapO-Canada and CapO-US conducted a marketing and credit card campaign that was primarily designed and effected in the USA, and only secondarily in Canada, adopting the CapO Data Strategy. The Canada Campaign in Canada adopted the was directed by CapO-US in the name of CapO-Canada. The Canada Campaign had two primary business objectives: (i) the acquisition of credit card customers in Canada; and (ii) the acquisition and subsequent post-Single Use Purpose completion retention, storage, migration, internal and external use and unwarned increasing risk of a Data Breach regarding the Confidential Data from all persons (Class Plaintiffs) who applied for a credit card and consumer credit from CapO-Canada and its Partners.

32. The Canada Campaign involved a high saturation and high-cost marketing and technical strategy that represented a major investment of Capital One in Canada. As such, the subsequent improper retention, storage, migration, use and increasing exposure of data from a data breach of Confidential Data farmed from Canadian consumers including the Class Plaintiffs was an important hidden profit centre and strategic tool that was, *inter alia*, a significant factor in the success of the Canada Campaign and a profitable benefit to the five defendant corporations encompassed in the definition of Capital One in Canada and the US for all of their worldwide businesses.

33. In 2005, CapO-US incorporated a wholly owned and controlled its banking subsidiary in Canada being Capital One Bank (Canada Branch) and Capital One (Services) Canada Inc., collectively and previously defined as "CapO-Canada". Capital One Bank (Canada branch) sought a banking license from the primary Canadian regulator, the Office of the Superintendent of Financial Institutions Canada ("OSFI"). CapO-Canada received a license to operate as an authorized foreign bank pursuant to the *Bank Act* S.C., 1991, c. 46. This license permitted Capital One to conduct its credit card business in Canada through its Canadian branch, Capital One Bank (Canada Branch). OSFI regulated the new Canadian Bank. Capital One Bank (Canada Branch) was also regulated by the Financial Consumer Agency of Canada ("FCAC"), the Office of the Privacy Commissioner of Canada and the Financial Transactions and Reports Analysis Centre of Canada. Capital One, in all its emanations, operating directly or indirectly in Canada was and is subject to regulation under various Canadian federal laws, including: the *Bank Act* and its Regulations, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the *Personal Information Protection and Electronic Documents Act ("PIPEDA*").

34. Capital One's business decision to operate as a bank in Canada brought it into unfamiliar bank/customer and bank/potential customer obligations of absolute trust and fiduciary duties owed to all applicants, including the Class Plaintiffs. The fundamental change for Capital One was the limitations on the use of customer and potential customer assets, among them the Confidential Data ("Data Assets") and the accompanying individual, financial and personal profile of each customer or potential customer ("Financial Personality"). The retention, storage, migration, and use of the Data Assets beyond the Single Purpose Use was prohibited and represented an improper conversion of the Data Assets, a breach of trust and fiduciary duties owed by Capital One variously acting as banks, an intentional intrusion upon seclusion of the Class Plaintiffs, an intentional misappropriation of Financial Personality of the Class Plaintiffs, a breach of privacy rights and standards in Canada, and a breach of the section 8 privacy rights enshrined in the *Charter of Rights and Freedoms*.

35. As a bank registered in Canada, CapO-Canada and, to the extent that all of the corporate entities comprising Capital One were involved directly or indirectly in the business in Canada, were collectively bound by, *inter alia*, privacy; legislation, regulations, regulatory decisions, court decisions; consumer legislation and court decisions; other data protection laws, decisions and standards extant in Canada during Decades 1, 2 and 3 (the "Data Protection Laws and Standards"), mandating controls and terms of privacy protection and freedom from risk of harm to the Confidential Data of the Class Plaintiffs.

36. Under the Data Protection Laws and Standards, the corporations encompassed by the definition of Capital One, including CapO-Canada and CapO-US, were bound by PIPEDA, regulations promulgated and decisions made by the Privacy Commissioner under PIPEDA, Privacy Acts and Consumer Protection Acts listed in Schedule "A" (wherever relevant in Canada), court decisions involving privacy and consumer rights, the *Charter of Rights and Freedoms*, and recognized standards extant in Canada from time to time (forming part of the definition of Data Protection Laws and Standards). The Data Protection Laws and Standards, including, *inter alia*, the mandatory legal requirements and standards promulgated under PIPEDA (the "PIPEDA Laws and Standards") bind CapO-Canada and CapO-US regarding their treatment of the Confidential Data of the Class Plaintiffs.

37. Under the PIPEDA Laws and Standards, meaningful consent requires the observance of: (a) mandatory legal requirements; and (b) best practices ("Meaningful Consent").

38. The mandatory legal requirements embraced by the concept of Meaningful Consent under PIPEDA (part of the Data Protection Laws and Standards) and under the laws of Canada include:

(i) the primacy of data privacy and protection for Canadians delivering data to any third party organization;

(ii) in this case, CapO-Canada and CapO-US as the inducing and receiving bank of the Confidential Data of the Class Plaintiffs, must assess the nature of the data, as highly sensitive and related to security interests of the Class Plaintiffs in: receiving, retaining, using, migrating and protecting the Confidential Data;

(iii) Confidential Data sent by the Class Plaintiffs/applicants in this case is afforded the highest degree of sensitivity requiring CapO-Canada and CapO-US to abide by the most restrictive standards of use, and confine the use and further dealing with the Confidential Data to its Single Purpose Use;

(iv) the sensitivity and circumstances of the sending, receiving and use of the Confidential Data legally obliged CapO-Canada and CapO-US to hold the Confidential Data corporately in CapO-Canada and geographically in Canada on their Canadian servers dedicated to the protection of the Data during the Single Purpose Use, and thereafter the Confidential Data must be destroyed or returned to the Class Plaintiffs;

(v) the sensitivity and circumstances of delivery of the Confidential Data legally required

that any continuing retention and storage of the Data beyond the Single Purpose Use, any different use outside the Single Purpose Use, by CapO-Canada, including retention, storage, migration, use and exposure to risk of harm by third parties, be effected only after Meaningful Consent has been obtained for each and every retention, storage, migration, use or exposure to risk;

(vi) in any event, geographical and corporate migration required continuing notices and new Meaningful Consents that are informed, express, in writing and given after full disclosure, clear and easily accessible choices and allowing time and circumstance for independent advice;

(vii) the sensitivity and circumstances of the delivery of Confidential Data legally required that the nature and timing of any enforceable and binding Meaningful Consent be objectively viewed from the perspective of the Class Plaintiffs as a whole, having regard to the sensitivity of the Data and their aggregated level of sophistication and vulnerability of the Class Plaintiffs as a group;

(viii) the sensitivity and circumstances of delivery of the Confidential Data legally required that any increase in the residual risk of harm to the Confidential Data over time from Data Abusers be the subject of written individual notice to each Class Plaintiff, giving rise to a clear and comprehensible duty to warn each Class Plaintiff by CapO-Canada and CapO-US and an express direction and Meaningful Consent to continue to retain the Data in the face of the increased risk of harm;

(ix) the sensitivity and circumstances of delivery of the Confidential Data by the Class Plaintiffs legally required CapO-Canada and CapO-US to obtain Meaningful Consent before the Data was: (i) migrated from Canada to the USA; (ii) aggregated with other Data derived from persons other than the Class Plaintiffs who were applicants and customers of CapO-US; and/or (iii) migration in the aggregated data and/or solely as the Confidential Data to Amazon Web, thereby increasing the numeric significance of the Banking Data stored on the servers of Amazon Web and creating a data package of Confidential Information of 100 million persons, of extreme interest to data hackers; (iv) further increased risk of a data breach, publication and misuse by Data Abusers;

(x) in any event, the Confidential Data, wherever held and as migrated to a third party storage company at Amazon Web, imposed a duty variously on CapO-Canada, CapO-US, Amazon Web and GitHub to: (i) deliver an express notice to warn of any increasing risk of a data breach; (ii) complete, review and act on inter-company annual cross-internal and cross-external audits, risk assessments, technical reports on the respective corporate vulnerabilities regarding protection of the Confidential Data; and (iii) resolve any risks of a data breach by immediate joint action to correct and eliminate all vulnerabilities assessed, both as known and those that ought to have been known (the "Cross-Audit Program"); and

(xi) having regard to the sensitivity of the Confidential Data, in the case of a data breach, to immediately effect a notice program and amelioration program, including monetary compensation, delivered personally and in writing (through each form of notice and media available to effectively ensure delivery) to each Class Plaintiff.

39. Under the PIPEDA Laws and Standards, CapO-Canada and CapO-US were also required to meet best practices (part of the "Data Protection Laws and Standards") applicable to this action, namely:

(i) during any Data retention (wrongful though it was), CapO-Canada and CapO-US owed a duty to the Class Plaintiffs to periodically communicate with the Class Plaintiffs to remind them that their Confidential Data was being retained, stored, migrated, used and/or at increasing risk to a Data Breach and presenting them with options regarding the Confidential Data in those circumstances; and

(ii) during any Data retention (wrongful though it was), CapO-Canada and CapO-US owed a duty to the Class Plaintiffs to design and implement an interactive privacy communication protocol that permitted immediate and continuing communications between the Capital One entities and the Class Plaintiffs permitting real-time notifications to and directions from the Class Plaintiffs regarding any changes in the retention, storage, use, migration of and any residual increased risks of significant harm to the Confidential Data.

40. From January 1, 2005 to July 30, 2019 (the "Class Period"), at times and places throughout Canada, CapO-Canada and its Partners, on their own and through the Capital One Partners (variously through extensive mailings, direct contacts and advertisings in a variety of forms, the details of which are not presently fully known by the Class Plaintiffs), offered credit cards, consumer credit and other related banking services to Canadians. CapO-Canada and its Partners required that any interested Canadian was required to deliver their Confidential Data with their application. In answer to the invitation, six (6) million Canadians applied for credit cards issued by Capital One and/or its Partners ("Applicants"). In each and every application, the Applicants/Class Plaintiffs were required to deliver to CapO-Canada their Social Insurance Numbers ("SIN"), prior and existing banking arrangements, credit ratings, incomes, prior and existing credit cards, addresses, and telephone numbers ("Confidential Data").

41. By 2005, CapO-US had decided to extend its business into Canada. CapO-US and CapO-Canada began their credit card and data farming strategy in Canada under the auspices of Capital One Bank (Canada Branch), the wholly owned Canadian subsidiary and bank branch, CapO-Canada, as a bank registered under the Bank Act promulgated by the Federal Government of Canada. By doing so, Capital One assumed bank/customer obligations of trust and fiduciary duties. These obligations of trust and fiduciary duties required CapO-Canada and CapO-US to maintain the Confidential Data/Data Assets/Financial Personalities in absolute and exclusive confidence of CapO-Canada. These obligations of trust and fiduciary duties include: (i) an obligation to use the Confidential Data only for the Single Purpose Use; and (ii) an absolute obligation to prevent and warn of an ever-increasing risk of harm of a Data Breach and subsequent publication and fraudulent use by Data Abusers. CapO-Canada and CapO-US were not entitled to convert to their own use, retain, store, migrate, use and/or expose to increasing risk of a Data Breach of the Confidential Data, Data Assets and Financial Personalities (the "Unauthorized Retention, Use of and Risk to Confidential Data") for any other purpose other than the Single Purpose Use. The continuing Unauthorized Retention, Use of and Risk to Confidential Data was in breach of the Banking Trust obligations to hold the Confidential Data, Data Assets and Financial Personalities in the highest confidence, avoiding the Unauthorized Retention, Use of and Risk to Confidential Data conversion, breach of trust and fiduciary duties, and an intentional breach of privacy rights of the Class Plaintiffs under the Data Protection Laws and Standards.

42. The Canada Campaign included marketing reports, business research reports, regulatory opinions, consumer research reports, potential interest rate charges and numerous other technical reports considered by the executives, and the Board of Directors of CapO-US before the Canada Campaign was launched. CapO-US and thereafter CapO-Canada targeted a high-volume, high interest rate offering that permitted Capital One to tailor consumer credit and credit cards to the requirements of each Class Plaintiff/Applicant. The consumers targeted and those who applied for a Capital One credit card and credit were made up of a large number of vulnerable consumers who would otherwise find it difficult to obtain credit and credit cards in Canada. The credit card was a highly desirable passport to consumer spending. Capital One knew of, targeted and desired to serve this vulnerable group of consumers.

43. The methods employed in Canada found in the IBS Strategy/CapO Data Strategy were high volume, high interest costs, and high risk. The risk to Capital One was ameliorated by, *inter alia*, the value inherent in and to be realized from the Unauthorized Retention, Use of and Risk to the Confidential Data. The Canada Data Strategy sought high profits, and lower costs and tolerated ever-increasing higher risks of Data Breach to and exposure of the Confidential Data of the Class Plaintiffs to Data Abusers.

44. The IBS Strategy allowed Capital One to successfully outmarket and compete against the much more established banking institutions and ultimately develop approximately 50-million customers in the USA and Canada. The Canada Campaign conducted by CapO-Canada and CapO-US attracted approximately 6-million Canadians who submitted their Confidential Data in their application for a credit card. From the date that the Single Purpose Use was spent for each Applicant/Class Plaintiff to today's date, the Confidential Data has been continuously and improperly subjected to the Unauthorized Retention, Use of and Risk to the Confidential Data for profit.

(b) Confidential Data – Collection and Permitted Analysis: Single Purpose Use

45. From 2005 to 2020 and thereafter, Capital One conducted the Canada Campaign by, *inter alia*, marketing and advertising broadly across Canada, encouraging Canadians to apply for credit cards being issued in the name of Capital One and its Partners. Capital One set up a program of marketing, providing standard form application documents and information requirements (Confidential Data) to the target potential applicants, a system of internal credit review, and analysis of Confidential Data enabling CapO-Can and CapO-US to decide which of the applicants would be invited to receive individualized credit cards and consumer credit. CapO-Can and CapO-US treated the Confidential Data received from the Class Plaintiffs/Applicants as their own assets to be retained, stored, migrated, used, and held regardless of increasing risk of harm of a Data Breach for their own indefinite and continuing pleasure and profit.

46. The Capital One marketing and advertising program under the Canada Campaign invited Canadians to apply for a Capital One or Capital One Partner credit card. The invitation required that each applicant deliver the Confidential Data to Capital One. In law, the Confidential Data was received in confidence and could only be used for the Single Purpose Use. The Single Purpose Use was spent as soon as the application was considered, declined or accepted by Capital One. The Confidential Data could only be retained and further used by Capital One if they obtained a separate Meaningful Consent to each step of: retention, storage, migration to USA, internal and external use and sale, migration to Amazon Web, and continuing retention of the Confidential Data in the face of increased risk of harm and loss to Data Abusers of the Data due to a Data Breach. Contrary to the actions of CapO-Canada and CapO-US, the defendants failed to obtain Meaningful Consent under the highest standards for confidentiality, trust and fiduciary duties pursuant to the Data Protection Laws and Standards and the Privacy Rights and Banking Trust obligations.

47. In the period 2005 to March 2019, CapO-Canada received applications from over 6 million Canadians. Of those 6 million Canadians who applied for a credit card from CapO-Canada, a smaller number of Canadians received and/or accepted and used credit cards of CapO-Canada and CapO-US (the exact numbers of Canadians involved is known to Capital One, but unknown to the Class Plaintiffs). Only those Class Plaintiffs who accepted and used credit cards of Capital One became customers of CapO-Canada and CapO-US.

48. From and after the date that the Confidential Data was received by CapO-Canada and possibly CapO-US from the Class Plaintiffs/Applicants, it was analyzed, considered for credit reliability and receipt of a credit card by one or all of Capital One in Canada or the USA (the details of which are unknown to the Class Plaintiffs) under the IBS System.

49. The Confidential Data was delivered to CapO-Canada from the Class Plaintiffs/Applicants for the Single Purpose Use of assessing the suitability of each Applicant for consumer credit and a credit card (the "Single Purpose Use") and for no other purpose regardless of whether the Class Plaintiff/Applicant became a customer/credit card holder of Capital One or its Partners. The corporate operating distinction between CapO-Canada and CapO-US is blurred so that it is presently impossible to detail which of the Capital One Defendants was responsible for the Single Purpose Use and thereafter responsible for the Unauthorized Retention, Use of and Risk to the Confidential Data.

50. At some point after the Confidential Data of each Class Plaintiff/Applicant was delivered to CapO-Can, it was migrated without authorization of the Class Plaintiffs achieved by Meaningful

Consent to the servers of and controlled by CapO-US. The Confidential Data then became under the control of one or both of CapO-Canada and CapO-US. The migration of the Data to the USA was an intentional breach of the Data Protection Laws and Standards and the Banking Trust obligations.

51. In any event, the Single Purpose Use of the Confidential Data was spent as soon as the first analysis for the purpose of credit worthiness and credit card approval, the authorized use of the Data was spent. Once spent, the Confidential Data had to be returned to the Class Plaintiffs within a reasonable time or destroyed (as directed), pursuant to the Data Protection Laws and Standards and the Banking Trust obligations.

52. Any retention, storage, migration, internal and external use and continuing exposure of risk to harm by Data Breach of the Confidential Data was an Unauthorized Retention, Use of and Risk to the Confidential Data.

53. Contrary to the Data Protection Laws and Standards, and the Banking Trust obligations, CapO-Canada and CapO-US variously at times and on servers unknown to the Class Plaintiffs retained all of the Confidential Data belonging to the Class Plaintiffs for variously more than fifteen years of the Capital One business in Canada as if the Confidential Data were an asset belonging to Capital One for their own pleasure and profit without regard to the increasing risk of a Data Breach and ultimately in the period March to August, 2019 exfiltration to Data Abusers causing and threatening to cause further distress, humiliation, anguish, damages, moral damages, that any reasonable person would consider 'highly offensive' arising from intentional and reckless conduct of CapO-Canada and CapO-US. The facts 'cry out for a remedy' arising from this intentional and/or reckless Unauthorized Retention, Use of and Risk to Confidential Data.

(c) Confidential Data – Retention, Storage, Migration to USA and Increasing Risk

54. Regardless of where the Confidential Data was first analyzed, retained, and subsequently stored, used, migrated in Canada or the USA (the details of which will be particularized at trial), the post-Single Purpose Use, retention, storage, migration, internal and external use of the Confidential Data by Capital One was an intentional breach of the Data Protection Laws and Standards and in the face of the known increasing risks of a Data Breach, a reckless breach of the Data Protection Laws and Standards, including an intentional and/or reckless intrusion upon seclusion of the privacy rights of the Class Plaintiffs and an intentional and/or reckless misappropriation of their Financial Personalities for the profit of Capital One. The continued retention, storage and migration of the Data in the face of increasing risks of a Data Breach was wrongful conversion of the Data, breach of the duty to warn, breach of the Banking Trust obligations, negligent and, alternatively, negligent breach of contract and breach of contract.

55. At the outset and during Decade 2, Capital One knew that there was an ever-increasing risk of a data breach, exposing the Confidential Data to unauthorized persons. Capital One knew that the data protection regulations in Canada were increasing, placing high privacy obligations on Capital One holding the Confidential Data. At the same time, Capital One operated its business on the basis that the retention of data was fundamental to its business model. The continued unauthorized retention and internal and external use of the Confidential Data became an increasingly profitable part of the enterprise during Decades 2 and 3. Capital One did not notify the Class Plaintiffs of the continued unauthorized use and profits drawn from the Confidential Data.

56. As Capital One was perfecting its use of personal and confidential consumer data beginning in 1994 and thereafter, advances in technology increasingly made during the three relevant decades increased value and use of the personal and financial data collected, maintained and exploited by Capital One, including the Confidential Data. The dark side of this technological revolution was the ever-increasing risk of unauthorized access to data by the Data Abusers more easily and quickly disseminated to individuals seeking to damage class plaintiffs by misusing the Data. Each day that passed after the improper retention of the data of the Class Plaintiffs by Capital One increased the risk of a data breach and unauthorized access to the data, including the Confidential Data by Data Abusers.

57. Capital One knowingly, intentionally and recklessly failed to give regular and meaningful notice to the Class Plaintiffs of the retention, migration, storage and internal and external use of the Confidential Data by Capital One and the increasing risk to the Confidential Data from unauthorized migration of and increased risk of access to the Data by Data Abusers.

58. Throughout the three Decades in question, Capital One directly and indirectly made increasing profits from Confidential Data of the Class Plaintiffs without their knowledge. The profits arose from sale of the Confidential Data to third parties for, *inter alia*, use in market analysis, identification of individual consumer preferences, relationships with airlines for travel rewards and other programs not presently known by the Class Plaintiffs. Capital One was in breach of its Banking Trust obligations, duty of care, duty to warn and Data Protection Laws and Standards to give notice to the Class Plaintiffs of the direct and indirect use of the Confidential Data to enhance the profitability of Capital One. The notice obligations required that Capital One ask the Class Plaintiffs to renew their consent to the retention, storage, migration and use of the Confidential Data for profit at each significant change in the location and use of the Data and certainly in the face of increasing risks of a Data Breach. Capital One failed to do so. Capital One thereby breached the Data Protection Laws and Standards, was in breach of the laws of Canada, and intentionally invaded the privacy of the Class Plaintiffs, intentionally intruding upon their seclusion, intentionally misappropriating their Financial Personalities, intentionally invading their privacy rights recognized by section 8 of the *Charter of Rights and Freedoms* and committing the tort of conversion of the Confidential Data.

59. After the Confidential Data was migrated to the USA and placed under the unauthorized control of CapO-US and stored on their servers in the USA, CapO-US with the consent of CapO-Canada intentionally aggregated the Confidential Data of six million Canadian Applicants/Class Plaintiffs with the Confidential Data of approximately 94 million other applicant customers of CapO-US in the same or connected servers of CapO-US at times unknown to the Class Plaintiffs. The aggregation of all this Confidential Data of 100 million persons made the Class Plaintiffs' Confidential Data a 'target of targets' for the Data Abusers, thereby exponentially increasing the risk of a Data Breach. The aggregation of the Data was an intentional and/or wholly reckless Unauthorized Retention, Use of and Risk to Confidential Data in breach of Capital One's obligations to protect the privacy and safety of the Confidential Data.

60. Because of the wrongful retention, storage, use, and aggregation of the Confidential Data in the period March to August, 2019, Data Abusers exfiltrated and published the Confidential Data to the world causing and threatening to cause further distress, humiliation, anguish, damages, moral damages, that any reasonable person would consider 'highly offensive' arising from intentional and reckless conduct of CapO-Canada and CapO-US. The facts 'cry out for a remedy' arising from this intentional and/or reckless Unauthorized Retention, Use of and Risk to Confidential Data.

(d) Confidential Data – Use and Misuse for Profit

61. In the post-Single Purpose Use period, Capital One wrongfully used the Confidential Data for unauthorized analysis and profit to: (i) market existing and new services to all of Capital One's customers, including the Class Plaintiffs, as a group; (ii) market their existing and new services, including credit cards, to other potential applicants in Canada, the USA and the world; (iii) employed the Confidential Data for other unauthorized purposes and analysis connected with the business of Capital One but presently unknown to the Class Plaintiffs; and (iv) sell the Confidential Data as aggregated to third party external users for profit ("Unauthorized Uses").

62. The Unauthorized Uses were misappropriated by Capital One for its own corporate growth and profit in breach of the Data Protection Laws and Standards, the obligations within the Banking Trust and, in particular, intentional and/or reckless unauthorized intrusion upon seclusion and misappropriation of Financial Personalities and the charter rights of privacy under section 8 of the *Charter of Rights and Freedoms*.

63. Thus ended Decade 2 with CapO-US and CapO-Canada deeply and continuously involved in intentional and reckless conduct and seeking corporate profits using the Confidential Data at the

expense of rights and obligations owed to the vulnerable Class Plaintiffs and unknowingly facing increasing risks to their Confidential Data, which would soon arise, *inter alia*, from such conduct and be fatefully realized in the 2019 Data Breach and publication of the Confidential Data to the world and Data Abusers.

Decade 3 – 2015 to Date

Introduction

64. During Decade 2, Capital One suffered and recovered from economic and banking set-backs in a worldwide banking induced recession which commenced in 2008 and lasted until approximately 2011. In the recovery period after 2008, competitive and financial pressures arose from new banking capital and other requirements and regulations which increased costs and decreased profits of banks generally and Capital One in particular.

65. During Decade 3, the value and importance of data increased even more. Capital One leveraged its information technology to achieve its heightened profitability. A key part of its strategic focus included a reliance on third party outsourcers to help Capital One deliver its systems and operational infrastructure, *inter alia*, Amazon Web for its cloud infrastructure.

66. In this context, Capital One migrated a number of its core systems and consumer facing applications to Amazon Web as a third-party cloud infrastructure platform. Capital One did so, recognizing that unless the new environments were well managed, secure and effective that it could experience unplanned service disruption, system breakdowns and cyber-attacks which would have a material and adverse effect on the business and reputation of Capital One. Capital One recognized that the movement of data, including the Confidential Data, increased Capital One's risk exposure and the risk exposure of its customers. Every day that Capital One and Amazon Web wrongfully held the Confidential Data in storage increased the risk that an unauthorized person or persons would infiltrate, infiltrate and publicly use the Confidential Data for improper purposes to the high embarrassment of and damage to the Class Plaintiffs.

(a) Profit, Aggregation and Migration to Amazon Web: Increasing Risk

67. One of the ways to decrease costs and return to higher profits was, inter alia, to outsource data storage to the third-party cloud storage company, Amazon Web in 2015.

68. Other darker forces relevant to the ultimate Data Breach that stand as significant in this case are: (i) the increasing importance of data generally, and particularly the importance of highly sensitive financial data of the kind represented by the Confidential Data owned by the Class Plaintiffs; (ii) the radically increasing sophistication and appetite of Data Abusers as the Confidential Data (enhanced by its aggregation with 94 million other bank applicants and customers), became more valuable and therefore more vulnerable to the fraudulent intentions of Data Abusers; and (iii) the resulting exponential increase in the risk of a Data Breach affecting the Confidential Data and subsequent public exposure of the Data and damages to the Class Plaintiffs from the various and 'long-tail' fraudulent activities of Data Abusers.

69. Amazon Web's computer system contained known fundamental flaws ("Amazon Web's Flaws"). Capital One's computer system contained its own misconfiguration at the time the Amazon Web/Capital One cloud storage contract and transfer of confidential data occurred. Both Amazon Web and Capital One knew or should have known about this misconfiguration. The misconfiguration error occurred at an application layer of a firewall installed by Capital One (at times and places unknown to the Class Plaintiffs). The misconfiguration error was exacerbated by permissions set by Capital One that were broader than intended ("Capital One's Flaws").

70. The Amazon Web/Capital One (the "Contracting Parties") contract was the first and world's foremost contract for data storage and retrieval in the world. As such, it required special attention to and repair of the Amazon Web Flaws and the Capital One's Flaws before any Data was migrated

from Capital One to Amazon Web. The failure to repair the combined flaws in the computer systems and servers of the Contracting Parties was a breach of duty to care owed to, *inter alia*, the Class Plaintiffs respecting their Confidential Data.

71. The continued unauthorized and improper retention, storage and migration from Amazon Web multiply the risk of a Data Breach because of known technical computer vulnerabilities in Capital One servers and in Amazon Web servers which together increased the risk of a Data Breach. Neither Capital One nor Amazon Web took care to protect the Class Plaintiffs and the Confidential Data from the Data Breach because of increased costs inherent in the analysis and reconfiguration of their servers, and as hereinafter set out. These failings represented an intentional and reckless actions by Capital One and Amazon Web and unconscionably contributed to the increased risk of a Data Breach exposing the Confidential Data of the Class Plaintiffs to Data Abusers.

72. At the same time, the entire credit card business and other credit businesses came under increasing competitive pressures forcing continuing cost reductions so that Capital One could maintain its profitability and its vaunted profitability per share in the securities marketplace. To increase profits of Capital One in or about 2015, CapO-US and CapO-Canada decided on a bold and risky plan of cost reduction. The plan involved a migration of the aggregated data of 100 million bank applicants and customers, including the six million Canadian Class Plaintiffs, under the Capital One/Amazon Web storage contract.

73. While this Capital One/Amazon Web storage contract decreased the costs of Capital One and therefore increased their profits, it exponentially added to the risk of a Data Breach. It was an intentional and reckless act of corporate arrogance and self-interest. The migration of storage to Amazon Web was conceived by CapO-US and CapO-Canada executives and approved by its Board of Directors who variously owned shares of Capital One and stood to benefit personally from the decreased costs and resulting increased profits.

74. Capital One knew or ought to have known about the Capital One Flaws in their storage retention computer system and storage access computer system that existed before and at the time and after the execution of the Capital One/Amazon Web storage contract. Amazon Web knew or ought to have known of the Amazon Web Flaws in its cloud storage computer system and data access computer system. The migration of the Confidential Data from Capital One to Amazon Web therefore magnified the risk that the Confidential Data would be the subject of a Data Breach, exfiltration, publication, and misuse by Data Abusers.

75. The migration of the Confidential Data from the servers of CapO-Canada through other migrations of the Data to the USA to the servers of Amazon Web for misuse, cost reduction and profit in the face of exponentially increased risks as directed by the Capital One corporations, their executives and authorized by the directors of the Capital One corporations for cost reductions and resulting increased corporate and individual profits was 'highly offensive to any reasonable person', giving rise to intentional and/or reckless conduct for liability, damages, moral damages, punitive and aggravated damages and an order of aggregated damages under the relevant Class Proceedings Acts for the intentional conduct (as set out above) leading to greater data risk and ultimately unprotected losses arising from the Data Breach. The Data Breach was an intentional and/or reckless outcome leading inevitably to the Data Breach and infusing the Data Breach with intentional and reckless conduct by the corporate emanations of Capital One and Amazon Web. The corporate conduct of all of the Capital One corporations and the Amazon Web corporations was egregious.

76. Amazon Web was obliged to be assured that the Confidential Data was an asset of Capital One such that the Data could be legally migrated to the servers of Amazon Web. Amazon Web failed to obtain any independently verified assurance that the Confidential Data belonged to Capital One. Indeed, Capital One was unable to honestly give such an assurance to Amazon Web. Amazon Web failed to obtain the authorization from the Class Plaintiffs for the storage of the Confidential Data. In any event, Amazon Web, by accepting that Capital One owned the Confidential Data as its own asset, legally adopted all of the Capital One duties of care, duties to warn, and legal and customary obligations listed above and encompassed in the Data Protection Laws and Standards of the privacy

rights and Banking Trust obligations owed by Capital One to the Class Plaintiffs.

(b) Technical Computer Storage System Flaws – Amazon Web and Capital One

77. At the outset of the Capital One/Amazon Web storage contract in or about 2015 and during the contractual arrangement, the Chief Executive Officers ("CEOs"), Chief Financial Officers ("CFOs"), Chief Technology Officers ("CTOs") and Chief Risk Officers ("CROs") or their equivalents at Amazon Web and Capital One were together required (by internal and external experts, as required) to regularly and annually ensure that each corporation reviewed and approved the other's internal and external audit of computer information confidentiality standards and risk management procedures regarding the privacy and confidentiality of the Confidential Data in such a manner that it met the Data Protection Laws and Standards regarding computer information confidentiality. The committees of the Boards of Directors of each of Amazon Web and Capital One responsible for internal and external audit, risk and public reporting ought to have met, identified, examined and reported upon the deficiencies of the technical systems and, in particular, the Amazon Web Flaw and the Capital One Flaws (collectively, the "Flaws"). The relevant officers and members of the Boards of Directors failed in their obligations to expose and correct the known Flaws and other flaws affecting the security preservation and privacy of the Confidential Data in the computer systems of both enterprises (which other flaws are not now known to the Class Plaintiffs).

78. The Amazon Web cloud storage system suffered from a longstanding and well-known flaw, the server-side request forgery flaw ("SSRF") which compromised the security of the Confidential Data and (along with other failings and flaws) and contributed to the infiltration, exfiltration and worldwide publication of the Confidential Data taken from the servers of Amazon Web. The Amazon Web cloud computer system had other technical flaws (unknown to the Class Plaintiffs) which may have contributed to the wrongful access to, exfiltration of and publication of the Confidential Data to the world.

79. Amazon Web was obliged to inform Capital One of the SSRF flaw and other flaws, and correct them or provide for and insist upon further protections to Capital One to protect against the infiltration, exfiltration and publication of the Confidential Data by Data Abusers. In any event, Capital One knew or ought to have known of the SSRF flaw. In addition, Amazon Web neglected to and Capital One failed to insist that Amazon Web place a header on its system to protect the metadata service from data attacks and breaches using the SSRF flaw.

(c) Failed Mutual Obligations – Capital One and Amazon Web

80. Amazon Web had developed for purchase by its direct customers (including Capital One) several computer protection services that it could have employed to ameliorate against the SSRF Amazon Web Flaw and thereby protect the security and privacy of the Confidential Data, including: AWS Web Application Firewall; the service called Macie (which automatically classifies data into different buckets of sensitivity and then sends customer alerts if an anomalous requester tries to access the Confidential Data or if there is an unusually high volume of Confidential Data being moved); the service called GuardDuty (that alerts customers when there are unusual Application Programming Interface ["API"] calls); the service called Well Architected Review (where Amazon Web inspects a customer's technology architecture and gives feedback that the customer is well-architected according to best practices); and other security practices and layers (which Amazon Web was capable of providing to Capital One, including sub-systems deep in the technology stack that, if used, at the tail end of a lot of security layers to protect themselves). Amazon Web failed to review or properly review the Capital One computer system and insist that Capital One employ Amazon Web recommendations to protect the Confidential Data.

81. Additionally, Capital One and Amazon Web failed to rigorously, regularly and annually test its security measures, back-up and recovery systems and those of its third-party service providers. Capital One failed to sufficiently perform the required variety of vulnerability and penetration testing on its networks, platforms, systems and applications. Capital One and Amazon Web did not even repair or mitigate against their own known system flaws. In this regard, the executives at

Capital One and Amazon Web, including their CEOs, the risk management officers, their Chief Financial Officers, their technology officers, and their respective board of director committees entirely failed to protect the Confidential Data from cyber-attacks. At no time over the four years of the Capital One/Amazon Web storage contract did the corporations warn the Class Plaintiffs of the Amazon Web Flaws and the Capital One Flaws and the protections available to ameliorate against these flaws, and the ever-increasing risks of a Data Breach affecting the Confidential Data. At no time did Capital One and Amazon Web give the Class Plaintiffs a legally required notice about the migrations of the Confidential Information, the increasing risks of a Data Breach and a warning allowing the Class Plaintiffs to protect and manage risks to their Data Assets/Confidential Data, and risk of misappropriation of their Financial Personalities.

82. As a result, Capital One and Amazon Web fundamentally failed in their mutual obligations to the Class Plaintiffs in designing, effecting change and operating their computer storage systems and data retrieval systems under the Capital One/Amazon Web storage contract. These mutual failings further represent failures by Capital One and Amazon Web to abide by their duty to warn, duty of care, duty of trust and fiduciary duties, duty to protect against privacy breaches owed to the Class Plaintiffs. By these mutual failings, Capital One and Amazon Web have unconscionably, intentionally and recklessly allowed the intrusion upon the seclusion of the Class Plaintiffs and allowed their Financial Personalities to be misappropriated by Data Abusers, causing moral damages, and damages to the Class Plaintiffs claimed and as further particularized in this claim.

83. By failing to detect and correct the Capital One and Amazon Web flaws, the corporations, and their executives and Boards of Directors, fell below the standards expected of them placing the Confidential Data at increased risk of being accessed by the Data Abusers and causing damages to the Class Plaintiffs. Capital One and Amazon Web were therefore in breach of their duty of care to the Class Plaintiffs and negligent to them.

84. By reason of the above, Capital One and Amazon Web committed the wrongful conversion of the Confidential Data, the breach of confidence, trust and fiduciary duties owed, the duty to warn owed and duty of care owed by Capital One and Amazon Web and have caused damage to the Class Plaintiffs and for which they are liable for negligence, alternatively negligent breach of contract, intentional and reckless intrusion upon seclusion and misappropriation of Financial Personality, breach of trust and fiduciary duties, and breach of duty to warn.

85. The conduct, inaction and breaches set out above of Capital One and Amazon Web are highly offensive to any reasonable person and caused the Class Plaintiffs damage in the form of increased risk and ultimately their loss of privacy. Capital One and Amazon Web failed in their duty to live up to the Data Protection Laws and Standards. Capital One and Amazon Web carried out their breach of privacy and negligence with a view to increased profits. Capital One and Amazon Web failed to protect the section 8 rights ensured in the *Canadian Charter of Rights and Freedoms* and failed to live up to the reasonable expectations that they would protect the privacy of each and every Class Plaintiff.

(d) Thompson – Infiltrates Amazon Web Servers, Exfiltrates and Publishes Confidential Data

86. As part of their duty of care and other obligations of trust, confidence, and fiduciary duties, Amazon Web and Capital One owed a further duty of care in the hiring and permanent supervision of employees who were entrusted with access to the Confidential Data on the servers of both enterprises. Amazon Web and Capital One fell below the Data Protection Laws and Standards expected of them in storing and using the Confidential Data by employing and failing to properly supervise before and after her employment at Amazon Web, Paige Thompson ("Thompson") as a computer engineer responsible for or having access to the Amazon Web cloud computer servers and the computer servers of Capital One which stored and gave access to the Confidential Data of the Class Plaintiffs.

87. Thompson was employed by Amazon Web in the years 2016 to 2018 (the exact times and terms of the employment contract are not known to the Class Plaintiffs). The Amazon Web cloud computer

system had an SSRF vulnerability which compromised the security of the Confidential Data and (along with other failings and flaws) permitted the infiltration, exfiltration and publication of the Confidential Data held on its servers. The Amazon Web computer systems and servers had other flaws which permitted the wrongful infiltration of its systems and servers, exfiltration of the Confidential Data and subsequent publication on the servers of GitHub of the Confidential Data to Data Abusers.

88. By computer system design and operation failings, including the Amazon One Flaw and Capital One Flaws, Thompson was able to infiltrate the Amazon Web cloud servers which stored the Capital One data including the Confidential Data of the Class Plaintiffs. Thompson exfiltrated the Confidential Data. Thompson published the data to the world by placing it on GitHub.

89. Thompson left the employ of Amazon Web sometime in 2018.

90. Beginning on or about March 12, 2019, and continuing in the months of March and April, Thompson attempted to infiltrate the Confidential Data stored in the servers of Amazon Web by exploiting the known SSRF vulnerability and Capital One's misconfiguration error at the application layer of the firewall installed by it, and using other computer system vulnerabilities and using her knowledge and experience gained as a computer engineer employed at Amazon Web. On April 21, 2019, Thompson was successful in infiltrating, and exfiltrating the Confidential Data of the Class Plaintiffs.

91. The Confidential Data extracted and copied by Thompson was listed in more than 700 folders or buckets of data belonging, inter alia, to the Class Plaintiffs. The Confidential Data included variously Class Plaintiffs'/Applicants': SIN, names, addresses, dates of birth, bank account numbers and credit history. The SINs were encrypted or tokenized. The remaining Confidential Data was not encrypted or tokenized. Thompson and others were able to and did break the encryption over the SINs, making them broadly available to Data Abusers and any unauthorized person with access to the internet.

92. By reason of the employment and lack of proper supervision of Thompson during and after her employment at Amazon Web, Capital One and Amazon Web fell below the Data Protection Laws and Standards expected of them. In so doing, Capital One and Amazon Web failed in their duty of care owed to the Class Plaintiffs and caused damage to them. Capital One and Amazon Web are therefore negligent and liable to the Class Plaintiffs for all damages flowing from the Data Breach described above, and the improper publication of the Confidential Data.

93. As described above, the increasing risk of a cyber-attack was realized at the instance of Thompson infiltrating the Capital One data stored on Amazon Web, exfiltrating the data and publishing the data on GitHub (as detailed below). The successful cyber-attack occurred relying upon inadequate security protections on the firewalls and other computer protection systems at Capital One and Amazon Web (the full technical description of the failures being unknown to the Class Plaintiffs).

94. Capital One, Amazon Web, Thompson and GitHub are vicariously liable for Thompson's breach of confidence, breach of trust, breach of privacy, intentional and/or reckless intrusion upon seclusion of the Class Plaintiffs, misappropriation of the identity of the Class Plaintiffs, conversion of the Confidential Data.

(e) GitHub – Publication to the World

95. GitHub provides web hosting and allows users to manage and store computer information on its page. Thompson posted the Confidential Data exfiltrated from the servers of Amazon Web onto a GitHub page which includes her name on or about April 21, 2019.

96. Upon posting the Confidential Data on GitHub, it became instantaneously available for review, copying, permanent retention, abuse and fraudulent activity, therefore becoming the vehicle

whereby the Confidential Data was exposed for permanent fraudulent activity by Data Abusers and therefore causing existing and ongoing damage to the Class Plaintiffs.

97. GitHub was required to review and assess its own website to ensure that confidential information was not published on its website. GitHub failed to take any steps to prevent or terminate the publication of the Confidential Data of the Class Plaintiffs published on its website beginning on April 21, 2019 and continuing to August 2019. GitHub owed a duty of care to the Class Plaintiffs to ensure that the Confidential Data was not placed on its website without the Meaningful Consent of the Class Plaintiffs. GitHub breached the duty of care and fell below any reasonable standards or standards at all to prevent the publication of the Confidential Data and used by Data Abusers. GitHub therefore caused the Class Plaintiffs damage and was negligent to the Class Plaintiffs.

(f) Capital One and Amazon Web – Failure to Detect

98. Capital One and Amazon Web failed to discover in a timely manner or at all the publication of the Confidential Data when it was exfiltrated from the Amazon Web servers by Thompson and published by Thompson to the world on GitHub. Capital One and Amazon Web were required under the Data Protection Laws and Standards to have computer security sufficient to immediately detect any intrusion or attempted intrusion into their computer systems and to immediately detect any wrongful taking of data from their computer systems including the Confidential Data. Capital One and Amazon Web wholly failed to develop and/or install any operating systems, risk management systems or early warning systems that immediately detected the attempted infiltration to and successful exfiltration of the Confidential Data from the Amazon Web servers by Thompson in March 2019, on April 21, 2019, or at any time until Thompson herself and other third parties announced the Data Breach to the world in June 2019.

99. In or about the period June 18, 2019 to July 17, 2019, Thompson announced her infiltration, exfiltration and publication of, inter alia, the Confidential Data on social media and other platforms (which platforms are unknown to the Class Plaintiffs). Capital One and Amazon Web negligently missed these social media posts. Capital One and Amazon Web knew or should have known about the Thompson publications but failed to have sufficient market and public analyses to discover the postings.

100. Capital One and Amazon Web failed to discover the infiltration, exfiltration and publication of the Confidential Data for almost three months, from April 21, 2019 to July 17, 2019. This failure illustrates the high degree of inadequacy of their computer protection systems. Such dramatic failures fall below any reasonable standards expected of them in maintaining the confidentiality of the Confidential Data. These actions and inactions by Capital One and Amazon Web caused damages to the Class Plaintiffs and were therefore negligent or, in the alternative, in negligent breach of contract to the Class Plaintiffs.

101. Capital One and Amazon Web owed a duty to warn the Class Plaintiffs of any unauthorized and wrongful infiltration of their computer systems and exfiltration and publication of the Confidential Data. The duty to warn imposed upon Capital One was consistently breached from the completion of the Single Purpose Use, through the migrations of the Data to servers in the USA and Amazon Web, arising from the increased security risk from Data Abusers for the entire period that the Confidential Data was improperly retained, stored and used and after the Data Breach in April 2019 through to the discovery of the Data Breach in July and August, 2019.

102. As soon as the Confidential Data was deposited to the servers of GitHub, GitHub owed a duty of care to, *inter alia*, the Class Plaintiffs to warn them that the Confidential Data had been exposed to the public and a duty of care to remove it immediately. GitHub wholly failed in this duty of care, causing the Class Plaintiffs damage.

103. The breach by Capital One, Amazon Web and GitHub of their duty to warn the Class Plaintiffs of the Data Breach and resulting publication allowed continuing and harmful access to the Confidential Data by Data Abusers for approximately four months, and therefore caused the Class

Plaintiffs damage and continues to cause damage to the Class Plaintiffs.

104. On or about July 29, 2019, Capital One issued a press release which obscurely revealed that the Confidential Data of 100-million applicants had been breached. The notice was a wholly inadequate warning of the Data Breach to the Class Plaintiffs amounting to a misrepresentation by Capital One to the Class Plaintiffs. It did not inform the Class Plaintiffs and/or each of them, being some 6 million Canadians, that their Confidential Data had been published to Data Abusers through the internet.

(g) Largest Bank Data Breach – USA Senate

105. The data breach involving the servers of Capital One and Amazon Web, and/or either of them, came to the attention of the committees of finance; banking, housing and urban affairs; health, education, labor and pensions; armed services; special committee on aging of the United States Senate. Capital One and Amazon Web were contacted by the US Senate on August 5, and 8, 2019, respectively. Amazon Web responded to the US Senate on August 13, 2019.

106. By August 13, 2019, Capital One had not fulfilled its promise made in the July 17, 2019 press release that it would notify affected individuals, including the Class Plaintiffs, of the Data Breach in a manner that would have come to the attention of each Class Plaintiff, or at all. Capital One has still not advised the 6 million Class Plaintiffs of the original improper conversion of the Confidential Data, the conversion of the data through transfer to the USA and subsequently through Amazon Web, the inadequate security on the computer systems of Capital One and Amazon Web, the failure of Capital One and Amazon Web to maintain and store the Data according to reasonable standards contained in Canadian legislation and in the industry, and the ultimate publication of the Confidential Data to the world through the internet. These failures amount to the breach of duty to warn, negligence, negligent breach of contract, breach of confidence, and breach of trust and fiduciary duties owed by Capital One and Amazon Web to each of the Class Plaintiffs/Applicants.

107. Members of the Senate of the USA demanded that Capital One and Amazon Web answer for the failures leading up to the cyber-attack and data breach of, inter alia, the Confidential Data. Capital One and Amazon Web blamed each other's technical failings for the data breach itself, for failing to detect the data breach after it occurred on April 19, 2019, for failing to give an effective duty to warn each of the Class Plaintiffs that their Confidential Data was now exposed to public viewing and misuse by all manner of misuse, criminal action and fraud.

108. Capital One and Amazon Web answered the demands of the USA Senate but failed to live up to their duties to inform each and every Class Plaintiff that their Confidential Data had been exposed to the public on the worldwide web.

109. Capital One and Amazon Web have failed to take the steps directed of them by the USA Senate and/or their regulators in the United States. Whatever steps they have taken, Capital One, Amazon Web and GitHub have failed in their duty to warn and communicate of the data breach.

(h) Failure to Regularly and Interactively Warn and Communicate with the Class Plaintiffs

110. Capital One did not regularly or inform at all the Class Plaintiffs that their Confidential Data had been migrated from Canada to the USA by Capital One or that it had been migrated to Amazon Web. Capital One did not regularly or inform at all the Class Plaintiffs that their Confidential Data was at high risk due to the movement of the Confidential Data from Capital One servers to the cloud servers of Amazon Web, that it did so to reduce Capital One costs and increase its profits. Capital One did not regularly or inform at all that the risks to their Confidential Data had increased due to continuing technical changes permitting Data Abusers to hack into storage data systems generally and, in particular, to those of Capital One and Amazon Web.

111. Capital One and Amazon Web owed a duty to warn the Class Plaintiffs of the ever-increasing risks, the cyber security attack when it occurred, the data breach when it occurred, and the

publication of the Confidential Data on the worldwide web. Capital One and Amazon Web failed in their duty to warn the Class Plaintiffs of the data breach and publication of their Confidential Data in a timely way or at all.

112. Capital One failed to report the data breach of the Confidential Data to their American and Canadian regulatory authorities listed above, including without limiting OSFI, the Privacy Commissioner and the USA Federal Reserve.

113. Capital One and Amazon Web were corporately embarrassed by the publication of the Confidential Data, but were more concerned with any damage to their corporate reputations and profits, thereby failing to act and warn the Class Plaintiffs of the breach and harm accruing to the Class Plaintiffs in the period March 22, 2019 to April 9, 2019.

(h) Liability and Damage Consequences

114. By reason of the facts set out above, Capital One and Amazon Web failed to adhere to the Data Protection Laws and Standards, the Banking Trust obligations and standards for data protection extant in Canada during Decades 2 and 3. The failures, actions, inactions, negligence, breach of contract, breach of duties to warn, trust and fiduciary duties, breach of privacy and consumer rights (including intentional and reckless intrusion upon seclusion and misappropriation of Financial Personalities) have caused damage to the Class Plaintiffs and each one of them. The damages for which Capital One, Amazon Web, Thompson and GitHub are liable include general damages, punitive damages, exemplary damages, aggravated damages and an award of aggregated damage under the Class Proceedings Acts and damages for causing and threatening to cause distress, humiliation, anguish, damages, moral damages, that any reasonable person would consider 'highly offensive' arising from the intentional and reckless conduct of CapO-Canada and CapO-US. The facts 'cry out for a remedy' arising from this intention and/or reckless Unauthorized Retention, Use of and Risk to Confidential Data by the defendants.

PART IV – LIABILITY UNDER THE CIVIL CODE OF QUEBEC

115. For residents of Quebec, the Class Plaintiffs plead that the conduct of the defendants is in breach of Articles 1457 and 1463 to 1464 of the *Civil Code of Quebec*, L.R.Q., c. C-1991. In communicating Personal Information to third parties, (i) without authorization under law; (ii) without consent, and (iii) for a purpose other than for which it was obtained, the defendants and each of them are liable to the Class Plaintiffs resident in Quebec pursuant to Articles 3, 35 and 37 of the Civil Code of Quebec.

116. The failures set out above fell below the Data Protection Laws and Standards demanded of Capital One and Amazon Web. Capital One and Amazon Web therefore breached their duty of care and duty to warn owed to the Class Plaintiffs and caused damage to the Class Plaintiffs. Capital One and Amazon Web are therefore liable in negligence for the damages caused to each Class Plaintiff. To the extent that there were contractual relationships between Capital One and any of the Class Plaintiffs, Capital One was in breach of contract and in negligent breach of contract to these Class Plaintiffs.

117. The defendants and each of them, in: conversion; negligence; alternatively; negligent breach of contract; breach of trust and fiduciary duties; breach of duty to warn; intentional and reckless intrusion upon seclusion and misappropriation of Financial Personalities; breach of privacy rights; and breach of consumer protection rights; owed to the Quebec Class Plaintiffs directly and indirectly allowed for the communication of Personal Information to be communicated to the public without the consent of the Class Plaintiffs for purposes which were not related to the reason for the delivery of the Information in the first place.

PART V – DAMAGES; REASONABLE FORESEEABILITY; AGGREGATE, EXEMPLARY, PUNITIVE AND MORAL DAMAGES

118. By the actions and breaches of duty, negligence and, alternatively, breach of contract of Capital One described above, Amazon Web, Thompson and GitHub, the defendants and each of them breached the privacy of the Class Plaintiffs by allowing their Confidential Data to be exposed to the world. The combined actions of the defendants started as soon as Capital One wrongfully retained the Confidential Data, continued as the Confidential Data was converted to the use and misuse by Capital One (for which Amazon Web is also responsible when it received, stored and exposed the Confidential Data to increased risk by Data Abusers). The actions and inactions of the defendants caused a breach of the Class Plaintiffs' privacy which was highly offensive to any reasonable person and beyond the reasonable expectations of the Class Plaintiffs. The actions and inactions of the defendants were an intentional intrusion upon the seclusion of the Class Plaintiffs and misappropriated their names and consumer details. In addition and in any event, the actions and inactions of the defendants were an intentional and/or reckless intrusion upon the seclusion and misappropriation of the Financial Personalities of the Class Plaintiffs.

119. By reason of the allegations set out in this Claim, the Class Plaintiffs and each of them have suffered reasonably foreseeable damages for which the defendants are responsible, namely: (i) ongoing, imminent, impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; (ii) loss of confidence in the banking and financial system; (iii) actual identity theft, crime, fraud and abuse, resulting in monetary loss and economic harm; (iv) loss of the value of privacy and the confidentiality of the stolen confidential data; (v) the illegal sale of the compromised data on the deep web black market; (vi) expenses and/or time spent on credit monitoring and identity theft insurance; (vii) time spent scrutinizing bank statements, credit card statements, and credit reports; (viii) expenses and/or time spent initiating fraud alerts; and (ix) decreased credit scores and ratings; (x) damages arising from distress, humiliation, anguish arising from the highly offensive acts of Capital One in converting the Class Plaintiffs' Confidential Data to Capital One's own use for profit and recklessly and intentionally exposing the Confidential Data to publication to the world, including Data Abusers by reason of the wrongful conduct, negligence and breaches described above.

120. The Class Plaintiffs and each of them have suffered other general and special damages, the details of which will be supplied at trial.

121. In the alternative, if a contract existed between Capital One and any of the Class Plaintiffs, Capital One was in breach of contract and in negligent breach of contract in maintaining, storing and using the Confidential Data after the Single Purpose Use was spent.

122. The Class Plaintiffs are entitled to an award of aggregate damages amounting to $20,000 per Class Plaintiff pursuant to the relevant Class Proceedings Acts (Schedule "A").

123. By reason of the above, Capital One is strictly liable to the Class Plaintiffs for all damages and losses sustained by them due to the breach of the confidentiality and security of and publication of the Confidential Data.

124. The Class Plaintiffs are entitled to exemplary and punitive damages in the amount of $100-million and moral and aggravated damages in the amount of $20,000 per Class Plaintiff.

125. The Class Plaintiffs are entitled to an accounting for profits made by Capital One, the Capital One Partners, and Amazon Web from the sale, use, fees and interest charges from the use of credit cards during the Class Period for each Class Plaintiff, and an Order that the profits be disgorged in favour of the Class Plaintiffs in addition to the heads of damage set out above.

126. The Class Plaintiffs are entitled to an order that the Confidential Data be returned to the Class Plaintiffs forthwith and removed from the servers of Capital One, Amazon Web and GitHub.

127. The Class Plaintiffs are entitled to an order for full indemnity costs of this action.

PART VI – LIABILITY, BEHAVIOUR MODIFICATION AND DAMAGES: AGGRAVATING FACTORS

128. Capital One, Amazon Web and GitHub have offered no or inadequate monetary compensation for the distress, humiliation and anguish suffered by the Class Plaintiffs for this data breach. They have showed no remorse for their intentional and reckless actions, inactions, conversion, breach of privacy, intrusion upon seclusion, misappropriation of economic personality, breach of trust, breach of fiduciary duty, breach of duty to warn, negligence and, alternatively, breach and negligent breach of contract. Capital One, Amazon Web and GitHub operated their business at the top of the technology and business world. They have given no indication of behaviour modification in the face of the worst banking data breach in history involving 100-million customers worldwide.

129. By reason of the banking/trust and Class Plaintiff vulnerability context of the conduct of Capital One, Amazon Web and GitHub, the imposition of moral damages, aggravated damages, exemplary damages, punitive damages and damages to protect the Class Plaintiffs into the future as they face the risk of further intrusion into their personal and financial private lives and security is magnified.

130. The context of the Capital One assault on credit cards and banking in Canada by converting highly confidential private data belonging to the Class Plaintiffs on which to base ever increasing profits for most of this Century is significant in the assessment of liability and behaviour modification in this action. The vulnerability of the Class Plaintiffs responding to a highly sophisticated marketing campaign for over fifteen years for the convenience and profitability of Capital One shareholders is a major factor in analyzing liability, damages and behaviour modification. The actions of Capital One are an assault and an attack on the privacy rights inherent in section 8 of the *Canadian Charter of Rights and Freedoms*.

131. In any event, and in the context and facts of the case pleaded and having regard to the intentional and reckless intrusion into the privacy of the Class Plaintiffs, Capital One, Amazon Web, GitHub and Thompson are strictly liable for all damages claimed by the Class Plaintiffs.

PART VII – LEGISLATION, JURISDICTION AND PLACE AT TRIAL

132. The relevant legislation is listed in Schedule "A" hereto.

133. The Class Plaintiffs plead and rely upon the following provisions of Rule 17 of the Rules of Civil Procedure in support of such service: 17.02 (f) – the contract was made in Ontario;17.02 (g) – the tort was committed in Ontario; and 17.02(p) – the defendant carries on business in Ontario, and 17.05 – service outside Ontario in relation to the defendant holding company in the United States.

134. The Class Plaintiffs propose that this action be tried in the City of Toronto, in the Province of Ontario.

SCHEDULE "A"

The Class Plaintiffs claim and rely upon the following statutes and Regulations:

[…]

The Plaintiffs rely on the following federal, provincial, and territorial, privacy statutes: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; *Privacy Act*, R.S.B.C. 1996, c. 373; *Privacy Act*, R.S.C. 1985, c. P-21; *Privacy Act*, R.S.N.L. 1990, c. P-22; *The Privacy Act*, C.C.S.M., c. P125; *The Privacy Act*, R.S.S. 1978, c. P-24; *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25; *Right of Information and Protection of Privacy Act*, S.N.B. 2009, c. R-10.6; *Access to Information and Privacy Act*, S.N.W.T. 1994, c. 20; *Access to Information and Privacy Act*, S.N.W.T. (Nu) 1994, c. 20; *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5; *Freedom of Information and Protection of Privacy Act*, R.S.P.E.I. 1998, c.

F-15.01; *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1; *Access to Information and Protection of Privacy Act,* R.S.Y. 2002, c. 1; and *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.

The Plaintiffs rely on the following provincial and territorial consumer protection statutes: *Consumer Protection Act*, 2002, S.O. 2002, Chapter 30, Schedule A; *Canada Consumer Product Safety Act,* S.C. 2010, c. 21; *Business Practices and Consumer Protection Act,* S.B.C. 2004, c. 2; *Consumer Protection and Business Practices Act,* S.N.L. 2009, c. C-31.1; *The Consumer Protection Act,* C.C.S.M., c. C-200; *The Consumer Protection and Business Practices Act,* S.S. 2013, c. C-30.2; *Consumer Protection Act,* R.S.A. 2000, c. C-26.3; *Consumer Product Warranty and Liability Act,* S.N.B. 1978, c. C-18.1; *Consumer Protection Act,* R.S.N.W.T. 1988, c. C-17; *Consumer Protection Act,* R.S.N.W.T. (Nu) 1988, c. C-17; *Consumer Protection Act,* R.S.N.S. 1989, c. 92; *Consumer Protection Act,* R.S.P.E.I. 1988, c. C-19; *Consumer Protection Act,* C.Q.L.R., c. P-40.1; and *Consumers Protection Act*, R.S.Y. 2002, c. 40.

The Plaintiffs rely on the following negligence statutes: *Negligence Act,* R.S.O. 1990, c. N.1; *Crown Liability and Proceedings Act*, R.S.C. 1985, c. C-50; *Negligence Act*, R.S.B.C. 1979, c. 298; *Contributory Negligence Act,* R.S.N.L. 1990, c. C-33; *The Tortfeasors and Contributory Negligence Act,* C.C.S.M., c. T90; *The Contributory Negligence Act,* R.S.S. 1978, c. C-31; *Contributory Negligence Act,* R.S.A. 2000, c. C-27; *Contributory Negligence Act,* R.S.N.B. 2011, c. 131; *Contributory Negligence Act,* R.S.N.W.T. 1988, c. C-18; *Contributory Negligence Act,* R.S.N.W.T. (Nu) 1988, c. C-18; *Contributory Negligence Act,* R.S.N.S. 1989, c. 95; *Contributory Negligence Act,* R.S.P.E.I. 1988, c. C-21; *Civil Code of Quebec,* L.R.Q., c. C-1991, art. 1457; and *Contributory Negligence Act,* R.S.Y. 2000, c. 42.

The Plaintiffs also rely on: *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1; *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40; *Bank Act*, S.C. 1991, c. 46; *Electronic Commerce Act*, 2000, S.O. 2000, c. 17; *Payment Card Networks Act*, S.C. 2010, c. 12, s. 1834; and *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

SCHEDULE "B"

The list of the defined terms and their definitions is as follows:

"Amazon Canada" –Amazon Web Services. (Canada) Inc.;

"Amazon USA" –Amazon Web Services Inc.

"Amazon Web's Flaws" – The fundamental flaws contained by Amazon Web's computer system.

"Amazon Web" – Amazon Web Services. (Canada) Inc. and Amazon Web Services Inc.

"API" – Application Programming Interface

"Applicants" – The 6 million Canadians that applied for credit cards issued by Capital One and/or its Partners.

"Breach of Banking Trust" – Collective term for breach of trust and breach of fiduciary duty.

"Breach of Privacy Rights" – Collective term for torts of conversion, intentional intrusion upon seclusion, reckless intrusion upon seclusion, intentional misappropriation of Financial Personality, reckless misappropriation of Financial Personality, and breach of a duty to warn.

"Canada Campaign" – An international business outreach in Canada planned by CapO-US in the latter part of Decade 1 (1993-2004).

"Capital One Financial" –Capital One Financial Corporation.

"Capital One Partners" – The contracting parties in Canada, including the Bay, Costco, and MasterCard between 2005 and 2019.

"Capital One's Flaws" – The misconfiguration error that was exacerbated by permissions set by Capital One that were broader than intended.

"Capital One" – Collectively CapO-Canada and collectively CapO-US entities, who are directly or indirectly wholly owned and/or controlled subsidiaries or entities of Capital One Financial.

"CapO Data Strategy" – The IBS strategy upon which data use was based, adopted into the Canada Campaign, and directed from the executive offices of CapO-US.

"CapO-Canada" – Capital One Bank (Canada Branch), Capital One (Services) Canada Inc.

"CapO-US" – Capital One, N.A., and Capital One Bank (USA), N.A.

"CEOs" – Chief Executive Officers.

"CFOs" – Chief Financial Officers.

"Class Period" – The period from January 1, 2005 to July 30, 2019.

"Class Plaintiffs" – The putative class plaintiffs that represent the class of persons in Canada who applied for credit cards between 2005 and 2019 and/or provided confidential financial and personal information to Capital One, or contracting parties in Canada, including the Bay, Costco, WalMart, JC Penney and MasterCard, and others unknown to the Class Plaintiffs, between 2005 and 2019.

"Computer and Data Revolution" – A technological, computer, and data revolution faced by the American financial institution industry between 1994 and 2005.

"Confidential Data" – Confidential financial and personal information provided by class of persons in Canada who applied for credit cards between 2005 and 2019, including bank account numbers, credit history, incomes, names, addresses, dates of birth, telephone numbers, and prior and existing credit cards.

"Contracting Parties" – Amazon Web/Capital One that entered into the world's first contract for data storage and retrieval in the world.

"CROs" – Chief Risk Officers.

"Cross-Audit Program" – A way to resolve any risks of a breach by immediate joint action to correct and eliminate all vulnerabilities accessed.

"CTOs" – Chief Technology Officers.

"Data Abusers" – The organized crime, perpetrators of fraud, hackers, terrorists, activists, formal and informal instrumentalities of foreign governments and other external parties.

"Data Assets" – The assets of customers and potential customers, including Confidential Data.

"Data Breach" – A data breach in March 2019 by Capital One in the USA involving the confidential data of 6 million Class Plaintiffs delivered in trust to CapO-Canada for a Single Purpose Use, migrated to the USA, and aggregated with the confidential data of another 94 million applicants who sent their confidential data to CapO-US.

"Data Protection Laws and Standards" – The banking, privacy, consumer protection laws, legislation, regulation, regulatory movings, court decisions, and data protection standards extant in Canada throughout Decade 1 (1994-2005), Decade 2 (2005-2015), and Decade 3 (2015 to date).

"ERRATIC" – The alternative internet name for defendant Paige A. Thompson.

"FCAC" – Financial Consumer Agency of Canada.

"Financial Personality" – The individual, financial, and personal profile of each customer or potential customer.

"Flaws" – Collectively known as the Amazon Web Flaw and the Capital One Flaws.

"GitHub" - Defendant GitHub, Inc.

"Giudice" – The representative Plaintiff of the putative class action, Rina Del Guidice, resides in Ontario and is a Capital One Canada and Capital One USA cardholder.

"IBS Strategy" – An information based strategy developed by CapO-US.

"Meaningful Consent" – Meaningful consent requires the observance of mandatory legal requirements and best practices under PIPEDA Laws and Standards.

"Negligence" – Tort of negligence.

"Negligent breach of contract" – Collectively known as breach of contract and negligent breach of contract (if a contract existed at all).

"OSFI" – Office of the Superintendent of Financial Institutions Canada.

"PIPEDA Laws and Standards" – The Data Protection Laws and Standards, including, among others, the mandatory legal requirements and standards promulgated under PIPEDA.

"PIPEDA" – Personal Information and Protection and Electronic Documents Act, RSC, 2000 c. 5.

"SIN" – Social Insurance Number.

"Single Purpose Use" - CapO-US invited applicants to share confidential data for the single purpose of assessing worthiness and eligibility for a credit card.

"SSRF" – A server-side request forgery flaw from which the Amazon Web cloud storage system suffered.

"Thompson" – The Defendant Paige A. Thompson is a computer systems engineer residing in the USA, and a former employee of Amazon Web and/or Capital One.

"Unauthorized Retention, Use of and Risk of Confidential Data" – unauthorized retention, use and risk to Confidential Data whereby the Defendants converted to their own use, retained, stored, migrated, used and/or exposed to increasing risk of a Data Breach of the Confidential Data, Data Assets, and Financial Personalities for any other purpose other than the Single Purpose Use.

"Unauthorized Uses" – The retention, storage, migration and selling of the Confidential Data as aggregated to third party external users for profit.

"Wood" – The representative Plaintiff of the putative class action, Daniel Wood, resides in Alberta and is a Capital One Canada and Capital One USA cardholder.

Schedule "B" – Compendium Flow Chart

A7365

CITATION: Del Giudice v. Thompson, 2021ONSC 5379
COURT FILE NO.: CV-19-00625030-00CP
DATE: 20210804

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

RINA DEL GIUDICE and DANIEL WOOD
Plaintiffs

- and -

PAIGE A. THOMPSON, CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (CANADA BRANCH), CAPITAL ONE (SERVICES) CANADA INC., CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., GITHUB, INC., AMAZON WEB SERVICES INC., AND AMAZON WEB SERVICES (CANADA) INC.
Defendants

REASONS FOR DECISION

PERELL J.

Released: August 4, 2021